National Aeronautics and
Space Administration

NSTS 22206
REVISION D
DECEMBER 10, 1993

Lyndon B. Johnson Space Center
Houston, Texas 77058

REPLACES
NSTS 22206
REVISION C

SPACE SHUTTLE

REQUIREMENTS FOR PREPARATION AND APPROVAL OF FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND CRITICAL ITEMS LIST (CIL)

REVISION LOG

REV LTR	CHANGE NO	DESCRIPTION	DATE
		BASELINE ISSUE (Reference: Level II PRCBD S40107A, dated 10/9/86).	10/09/86
A	5	REVISION A (Reference: Level II PRCBD S40107J, dated 05/04/88) also includes S40107H and Changes 1 thru 4.	05/04/88
B	7	REVISION B (Reference: Level II PRCBD S40107K, dated 07/26/88) also includes Change 6.	08/12/88
C	8	REVISION C (Reference: Level II PRCBD S40107Q, dated 11/9/89)	12/15/89
D	21	REVISION D (Reference: SSP DOC–150, dated 11/5/93) also includes Space Shuttle PRCBD S052730A; CAR S050643A; SSP DOC–057 and Changes 9 thru 20.	12/10/93

CHANGE SHEET

FOR

NSTS 22206 - Space Shuttle
Requirements for
Preparation and Approval of Failure Modes and
Effects Analysis (FMEA) and Critical Items List (CIL)

CHANGE NO. 31

Program Requirements Control Board Directive No. S061493A/(4-1), dated 3/21/01 and SSP DOC-497.(1)

April 12, 2001

Robert H. Heselmeyer
Secretary, Program Requirements
Control Board

CHANGE INSTRUCTIONS

1. Remove the following listed pages and replace with the same numbered attached pages:

Page	PRCBD No.
2-1	
2-2	SSP DOC-497
5-1	
5-2	S061493A

NOTE: A black bar in the margin indicates the information that was changed.

2. Remove the List of Effective Pages, dated January 15, 2001 and replace with List of Effective Pages, dated April 12, 2001.
3. Sign and date this page in the space provided below to show that these changes have been incorporated and file immediately behind the List of Effective Pages.

_____ _____
Signature of person incorporating changes Date

NSTS 22206 - Space Shuttle
Requirements for
Preparation and Approval of Failure Modes and
Effects Analysis (FMEA) and Critical Items List (CIL)

*Revision D (Reference PRCBD No. S052730A, dated 10/20/93; CAR S050643A, dated 11/23/93; SSP DOC-057 and SSP DOC-150)

LIST OF EFFECTIVE PAGES

April 12, 2001

The current status of all pages in this document is as shown below:

Page No.	Change No.	PRCBD No.	Date
i - ii	Rev. D	*	December 10, 1993
iii	22	S050107V	October 19, 1994
iv	Rev. D	*	December 10, 1993
v	24	S050107W	June 12, 1995
vi	29	S053983CKR1	February 2, 2000
vii	22	S050107V	October 19, 1994
viii	Rev. D	*	December 10, 1993
1-1	22	S050107V	October 19, 1994
1-2	Rev. D	*	December 10, 1993
2-1	29	S053983CKR1	February 2, 2000
2-2	31	SSP DOC-497	April 4, 2001
3-1	Rev. D	*	December 10, 1993
3-2	28	S061177	November 9, 1998
3-3 - 3-4	Rev. D	*	December 10, 1993
3-5 - 3-6	23	S050107T	November 20, 1994
3-6A	30	S053983CY	December 13, 2000
3-6B	23	S050107T	November 20, 1994
3-7 - 3-8	Rev. D	*	December 10, 1993
3-9	27	S060827AR1 SSP DOC-307	May 12, 1997, May 9, 1996
3-10 - 3-14	28	S061177	November 9, 1998
3-15	27	S060827AR1	May 12, 1997
3-16	28	S061177	November 9, 1998
3-17	27	S060827AR1	May 12, 1997
3-18	27	S060827AR1 SSP DOC-307	May 12, 1997, May 9, 1996
3-19	Rev. D	*	December 10, 1993

LIST OF EFFECTIVE PAGES

April 12, 2001

Page No.	Change No.	PRCBD No.	Date
3-20	23	SSP DOC-234	December 5, 1994
3-21 - 3-24	Rev. D	*	December 10, 1993
3-25 - 3-28	28	S061177	November 9, 1998
3-29 - 3-35	Rev. D	*	December 10, 1993
3-36	27	S060827AR1	May 12, 1997
3-37 - 3-38	Rev. D	*	December 10, 1993
4-1 - 4-2	Rev. D	*	December 10, 1993
4-3 - 4-4	23	S050107T	November 20, 1994
4-4A	25	S050107Y	August 31, 1995
4-4B	23	S050107T	November 20, 1994
4-5 - 4-11	Rev. D	*	December 10, 1993
4-12	25	S050107Y	August 31, 1995
4-13 - 4-15	Rev. D	*	December 10, 1993
4-16	25	S050107Y	August 31, 1995
4-17 - 4-18	Rev. D	*	December 10, 1993
5-1	29	S053983CKR1	February 2, 2000
5-2	31	S061493A	March 21, 2001
5-3 - 5-5	29	S053983CKR1	February 2, 2000
5-6 - 5-8	Rev. D	*	December 10, 1993
5-9	27	SSP DOC-307	May 9, 1996
5-10	24	S050107W	June 12, 1995
5-11 - 5-14	Rev. D	*	December 10, 1993

NSTS 22206

SPACE SHUTTLE

REQUIREMENTS FOR PREPARATION AND APPROVAL OF FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND CRITICAL ITEMS LIST (CIL)

THIS PAGE INTENTIONALLY LEFT BLANK

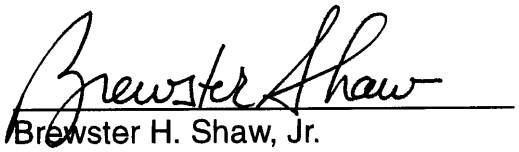
FOREWORD

Efficient management of the Space Shuttle Program (SSP) dictates that effective control of program activities be established. Requirements, directives, procedures, interface agreements, and system capabilities shall be documented, baselined, and subsequently controlled by SSP management.

Program requirements controlled by the Director, Space Shuttle Operations, are documented in, attached to, or referenced from Volume I through XVIII of NSTS 07700.

This document provides detailed instructions for the preparation of Failure Modes and Effects Analyses (FMEAs) and Critical Items Lists (CILs). It further defines and implements FMEA and CIL requirements contained in NHB 5300.4 (1D–2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, NSTS 07700, Volume V, Information Management Requirements, NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specification, and NSTS 07700, Volume XI, System Integrity Assurance Program Plan.

All elements of the SSP must adhere to these baselined requirements. When it is considered by the Space Shuttle Program element/project managers to be in the best interest of the SSP to change, waive or deviate from these requirements, an SSP Change Request (CR) shall be submitted to the Program Requirements Control Board (PRCB) Secretary. The CR must include a complete description of the change, waiver or deviation and the rationale to justify its consideration. All such requests will be processed in accordance with NSTS 07700, Volume IV, and dispositioned by the Director, Space Shuttle Operations, on a Space Shuttle PRCB Directive (PRCBD).



Brewster H. Shaw, Jr.
Director, Space Shuttle Operations

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

NSTS 22206

CONTENTS

TABLES

FIGURES

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide all Space Shuttle projects with consistent methods for the preparation, maintenance and publication of the Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL) as required by NHB 5300.4(1D–2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, Paragraph 1D301–3. This document also provides the requirements for the identification and preparation of the Critical Line Replaceable Unit (LRU)/Hardware List in accordance with NSTS 07700, Volume XI, System Integrity Assurance Program Plan.

1.2 SCOPE

The scope of the task described herein and in the controlling documentation shall be applicable to all Space Shuttle projects. Project responsibilities include all flight hardware and Government Furnished Equipment (GFE) and Ground Support Equipment (GSE) used at or common to the launch sites and landing sites (SLF, SLS, CLS, etc.) and which interface with flight hardware. Flight hardware requirements are contained in Section 3.0. GSE FMEA/CIL preparation requirements are contained in Section 4.0. Current “as–built” configurations shall be used as the basis for the analysis.

1.3 GENERAL METHODOLOGY FOR FAILURE MODES AND EFFECTS ANALYSIS/ CRITICAL ITEMS LIST

In the process of conducting a FMEA, each hardware item is analyzed for each possible failure mode and for the “worst case” effect. The analyst begins the analysis with block diagrams which illustrate the operation, interrelationships, including software, and interdependencies of functional entities of a system and provide the ability for tracing failure mode effects through all hardware levels. Functional/reliability block diagrams are required to show the functional flow sequence and the series dependence or independence of functions and operations. Block diagrams should be constructed in conjunction with and after defining the system and should present the system as a breakdown of its major functions. More than one block diagram may be required to display alternative modes of operation, depending upon the definition established for the system. Those failure modes requiring retention rationale (reference Paragraph 3.3.2 for CIL Criteria for Flight Hardware and Paragraph 4.2c for the definition of GSE Critical Items), are formally documented. All other failure mode worksheets will be documented and retained as worksheets.

The process of conducting the FMEA includes the following:

a. Defining the system and its performance requirements.

b. Specifying the assumptions and groundrules to be used in the analysis.

c. Developing block diagrams or other simple models of the system.

d. Devising the analysis worksheet and completing for every identified failure mode. The effects documented address the worst case.

e. Recommending and evaluating corrective actions and design improvements.

f. Summarizing the analysis in report form.

Analysis results are documented by listing each identified failure mode for each component in the system being analyzed on a separate table or worksheet. The worksheet contains all data elements to be addressed in the analysis. The failure effects, causes, criticalities, etc., are individually assessed for each failure mode on each component depending upon the function that component performs.

2.0 APPLICABLE DOCUMENTS

The following documents of the date and issue shown form a part of this document to the extent specified herein. "(Current Issue)" is shown in place of the specific date and issue when the document is under Space Shuttle PRCB control. The current status of documents shown with "(Current Issue)" may be determined from NSTS 08102, Program Document Description and Status Report.

NSTS 07700 Volume IV (Current Issue)	Configuration Management Requirements
	Ref. Foreword, Para. 5.1
NSTS 07700 Volume V (Current Issue)	Information Management Requirements
	Ref. Foreword, Para. 3.3.6, 4.3.4, 5.2.1, 5.3.2
NSTS 07700 Volume X (Current Issue)	Space Shuttle Flight and Ground System Specification
	Ref. Foreword, Para. 3.2, 3.4.1, 3.4.8, 4.2, 5.1
NSTS 07700 Volume XI (Current Issue)	System Integrity Assurance Program Plan
	Ref. Foreword, Para. 1.1
NSTS 08080–1 (Current Issue)	Space Shuttle Manned Spacecraft Criteria and Standards
	Ref. Para. 3.4.1, 4.4.1, Figure 5–2
NSTS 08126 (Current Issue)	Problem Reporting and Corrective Action (PRACA) System Requirements
	Ref. Para. 3.4.10

NSTS 08399 (Current Issue)	Space Shuttle Program (SSP) Critical Items List (CIL) Ref. Para. 5.2.2
NSTS 16007 (Current Issue)	Shuttle Launch Commit Criteria and Background Document Ref. Para. 3.4.1
JSC 18206	Shuttle Data Integration Plan Ref. Para. 3.4.8
NHB 1700.7A	Safety Policy and Requirements for Payloads using the Space Transportation System Ref. Para. 3.2
NHB 5300.4 (1D–2)	Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program Ref. Foreword, Para. 1.1, 3.1, 4.1
NSS/GO–1740.9	NASA Safety Standard for Lifting Devices and Equipment Ref. Para. 4.5.1

3.0 INSTRUCTIONS FOR FLIGHT HARDWARE FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND CRITICAL ITEMS LIST (CIL)

3.1 SCOPE

This section further defines and implements NHB 5300.4(1D–2) and provides the requirements and groundrules for performing FMEAs and preparing CILs on flight hardware, including Contractor Furnished Equipment (CFE), Government Furnished Equipment (GFE) and Payload Integration Nominal Cost Hardware (PINCH).

3.2 DEFINITIONS

These definitions are vital to an understanding and interpretation of the requirements and groundrules contained in this document and shall be used as the reference source for flight hardware FMEA and CIL terminology.

a. Component – A combination of parts, devices, and structures, usually self–contained, which perform a distinctive function in the operation of the overall equipment. A “black box” (e.g., transmitter, encoder, cryogenic pump, star tracker).

b. Correcting Action – An identification of actions, automatic or manual, which could be taken to circumvent the failure.

c. Critical Item – A critical item is defined as any one of the following:

   1. A Single Failure Point (SFP).

   2. An item which becomes Criticality 1 (or in the case of Orbiter, redesigns approved after February 1, 1992, which reduce the system redundancy for intact abort operations to less than that provided prior to the redesign [fail safe minimum] and new designs approved after February 1, 1992, which have less redundancy for intact aborts than for normal mission operations) during intact abort, except for the system causing the abort.

   3. A redundant hardware item where the second failure results in loss of crew or vehicle.

   4. A redundant hardware item in a life or mission–essential application where:

      (a) Redundant hardware item is not capable of checkout during the normal ground turnaround sequence (Redundancy Screen A).

      (b) Loss of redundant hardware item is not readily detectable in flight (Redundancy Screen B).

(c) All redundant hardware items can be lost by a single credible cause or event such as contamination (Redundancy Screen C).

d. Criticality

1. Functional Criticality – Categorization of the effect of loss of all redundancy (like and/or unlike) for a given function (see Table 3.1). Functional criticality for redundant items is based upon multiple failures which must occur to result in loss of the system or component function. Any hardware item in the failure scenario contributing to or resulting in the effect shall be considered as “redundancy” (like and/or unlike, operational and/or standby).

2. Hardware Criticality* – Categorization of the singular effect of the identified failure mode of a hardware item (see Table 3.2).

*Applicable to Space Shuttle Vehicle Engineering Office and EVA and Crew Equipment Office only.

e. Emergency System or Hardware – Any system or hardware item which is used only after a life–threatening situation has occurred because of prior failures or events. This excludes hardware which performs a function used during any nominal mission phase or during intact abort. Use of an emergency system must be initiated manually. Emergency systems include the following (as a minimum):

1. Remote Manipulator System (RMS) jettison

2. Ku–band antenna jettison

3. Smoke detection/fire suppression

4. Range Safety System on the External Tank (ET) and Solid Rocket Booster (SRB)

5. Payload bay door extravehicular tools

6. Crew escape system

f. Failure – The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

g. Failure Mode – A description of the manner in which an item can fail.

h. Fail–Operational – The ability to sustain a failure and retain full operational capability for safe mission continuation.

i. Fail Safe – The ability to sustain a failure and retain the capability to successfully terminate the mission.

j. Hazard – The presence of a potential risk situation caused by an unsafe act or condition.

k. Interface – The point or area where a relationship exists between two or more parts, systems, programs, persons, or procedures where physical and/or functional compatibility is required.

l. Kit – A temporary addition or modification to the Orbiter or its subsystems to satisfy unique requirements for a specific mission.

m. Loss of Mission

1. Early termination of a planned mission

2. Cancellation of deployment activities for any Class “A” or “B” free–flyer payload/experiment

3. Inability to capture and safely return to earth a retrievable Class “A” or “B” free–flyer payload or experiment

4. Loss of or inability to complete significant/primary mission objectives

n. Loss of Personnel Capability – Loss of personnel function resulting in inability to perform normal or emergency operations. Also includes loss of life or injury to the public.

o. Loss of Vehicle System – Loss of the capability to provide the level of system performance required for normal or emergency operations.

p. Line Replaceable Unit (LRU) – An item whose replacement constitutes the optimum organizational maintenance repair action for a higher indenture item, i.e., any assembly which can be removed and replaced as a unit from the system at the operating location.

q. Post–Landing Safing Operations – For the purposes of this instruction, post–landing safing operations are defined as those activities performed after landing to prepare the Orbiter for ground turnaround operations and includes the following:

1. Deservice and draining of hazardous fluids

2. Safing of unused ordnance

3. Application of ground power and cooling

4. Removal of potentially hazardous components

5. Removal of pods and payloads

6. Purging and venting of gases

7. Installation of protective covers

r. Prelaunch Operations – Prelaunch operations for propulsion and power subsystems are defined as all activities performed from the beginning of tank loading for each specific subsystem to SRB ignition. For all other subsystems, prelaunch operations include all activities performed from the start of main engine conditioning to SRB ignition. (For Space Shuttle Main Engine [SSME], prelaunch operations cease at ignition of the SSME.)

s. Pressure Vessels (Defined by NHB 1700.7A, Safety Policy and Requirements for Payloads using the Space Transportation System) – A container that stores pressurized fluids and:

1. Contains stored energy of 14,240 foot–pounds (19,310 joules) or greater based on adiabatic expansion of a perfect gas, or

2. Contains a gas or liquid which will create a hazard if released, or

3. Has a design limit pressure greater than 100 psi.

t. Redundancy – Multiple ways of performing a function.

1. Operational Redundancy – Redundant hardware items, all of which are fully energized during the subsystem operating cycle. Operational redundancy includes load sharing hardware items connected in such a manner that, upon failure of one item, the remaining redundant items will continue to perform the subsystem function. Switching out the failed item is not required.

2. Standby Redundancy – Redundant hardware items that are nonoperative (have no power applied) until they are switched into the subsystem upon failure of the primary item. Switching can be accomplished by either automatic or manual means.

3. Like Redundancy – Identical hardware items performing the same function.

4. Unlike Redundancy – Nonidentical hardware items performing the same function. Safety features which provide protection for specific failure modes are considered as unlike redundancy for that failure mode; i.e., relief valves which provide protection against overpressurization after failure of a regulator, transducers, and associated software which provide redline protection.

u. Single Failure Point (SFP) – A single item of hardware, the failure of which would lead directly to loss of life, vehicle, or mission. Where safety considerations dictate that an abort be initiated when a redundant item fails, that item is also considered a SFP.

v. Waiver – A written authorization, granted after the fact, for use or acceptance of an article which does not meet the specified requirements.

w. 1R Non–CILs – Functional Criticality 1R failure modes which exceed the NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specification, fail–safe requirement by being at least two–fault tolerant, and satisfy the NSTS 07700, Volume X, requirements for redundancy verification and separation of critical functions (i.e., pass redundancy screens).

3.3 FAILURE MODES AND EFFECTS ANALYSIS AND CRITICAL ITEMS LIST DATA CONTENT AND SCHEDULE

3.3.1 Failure Modes and Effects Analysis

Each element or prime contractor shall perform a FMEA and the resulting worksheets and supporting data (block diagrams, schematics, etc.) shall be retained by the element project.

3.3.2 1R Non–CILs

1R non–CIL information shall be included in the CIL. The information contained in this grouping shall meet the criteria of Paragraph 3.3.4a thru d and, as a minimum, contain data elements 1 through 18 as defined in Table 3.6 (rationale for acceptability is not required for 1R non–CIL items).

NOTE: For the Orbiter Project, this requirement is imposed on new major Orbiter system upgrades after November 10, 1994 and is not retroactive.

3.3.3 Critical Items List Criteria

The following classification of failure modes, as a minimum, shall be included in the CIL:

a. All Functional Criticality Category 1 and 2 items

b. All Functional Criticality 1R items where (1) first failure could result in loss of mission, or (2) next failure of any redundant item could cause loss of crew/vehicle

c. All Functional Criticality Category 1R and 2R items that fail one or more redundancy screens

d. All items where the required failure tolerance for an intact abort is not met, except for the system causing the abort

3.3.4 Critical Items List Content

A CIL, which is derived from the FMEA, shall contain the following information, sequenced as indicated:

a. Introduction – Provides concise statements on objectives of the report.

b. Scope – Describes major systems contained in the CIL and general information on what type of data is contained in the CIL.

c. Critical LRU/Hardware List – Provides (by subsystem) a listing of LRU part numbers, reference designator (if appropriate), LRU nomenclature, LRU highest level criticality, lower level part numbers identified by the FMEA and respective nomenclature (i.e., component or piece part level), failure mode number, quantity of items in the subsystem, and criticality for each FMEA/CIL number, indicating redundancy screen(s) failed as applicable. (See Table 3.5 for data elements and format.) The Critical LRU/Hardware List shall include all critical items in accordance with the criteria contained in Paragraph 3.3.2.

d. Analysis Results – This section contains the individual CIL pages describing actual analysis results. The CIL is comprised of items meeting the definition of a critical item contained in Paragraph 3.2c. The CIL pages will, as a minimum, contain data elements 3 through 20 defined in Table 3.6. This includes the CIL rationale for acceptability which identifies the rationale or justification for retaining critical items and is comprised of design, test, inspection, failure history and operational use data elements as a minimum.

3.3.5 Critical Items List Data Elements

The data elements for flight hardware CILs are defined in Table 3.6.

3.3.6 Schedule

The schedule for submittal of CILs and 1R non–CILs will be in accordance with NASA approved 1Rs (see NSTS 07700, Volume V, Information Management Requirements, 2SR–22).

3.4 ANALYSIS REQUIREMENTS AND GROUNDRULES

3.4.1 Preparation Scope and General Requirements

a. A FMEA shall be prepared on all hardware, except for structure*, the Orbiter Thermal Protection System (TPS), and passive vents and drains for mission phases from prelaunch operations through post–landing safing operations and during ferry flights of the STS regardless of the probability of occurrence for each failure mode. Analysis shall be performed on the as–built configuration.

*NOTE: The following shall not be considered as “structure;” therefore, a FMEA is required.

1. Pressure vessels, component housings which provide containment capability, fluid lines, rigid pipes and ducts, rupture discs, sliding joints, expansion joints, structural devices used to capture, mate or join and release or demate hardware items (i.e., mechanical structural fasteners [excluding screws, bolts, nuts and rivets] such as: quick release mechanical pins, cam lock fasteners, latches, clamps [excluding wiring clamps and ties], spring clips, or hasps), or load carrying members such as cranks or rods will be analyzed for structural failure. Rigid lines and ducts shall be analyzed separately for each different fluid. Special lines (e.g., mechanical bellows, flex lines, etc.) shall be analyzed individually.

THIS PAGE INTENTIONALLY LEFT BLANK

2. Structural hardware with moveable, pivoting, sliding, expansion, or otherwise flexible joints.

3. Items which have a single mechanical barrier between oxidizer and fuel/combustible gas.

4. Aerodynamically sensitive items on the ET and SRB.

5. Any crew compartment seal or pressure barrier, the failure of which would result in inability to maintain required pressure.

b. FMEAs shall be conducted to the component/black box level. For components/black boxes identified as containing Criticality 1 and 2 SFPs, the FMEA shall be conducted within the component/black box to the hardware level necessary to identify potential SFPs.

c. Those components that are Functional Criticality 3 in the electrical circuit may be contained on one FMEA for that circuit.

d. All pyrotechnic items shall be identified in the CIL according to the most severe effect. Electrically initiated ordnance and pyrotechnic items only shall also include those effects resulting from premature operation.

e. FMEAs/CILs shall be documented and submitted on wire harnesses, cables, and electrical connectors as follows:

1. SSME, ET, and SRB:

(a) Each electrical cable assembly shall be analyzed to identify and document Criticality Categories 1, 1R, 2, and 2R failure modes. The analysis shall include failure modes for open circuits, short circuits, and complete loss of connector.

(b) Applicable critical items not meeting system design requirements of NSTS 08080–1, Space Shuttle Manned Spacecraft Criteria and Standards, Standards 4B, 20A, and 32 shall be identified, documented with a standard program waiver request, and submitted for program consideration.

2. Orbiter and GFE:

(a) All connectors in Criticality 1R functions that do not meet the physical separation requirements of NSTS 08080–1, Standard 20A and Criticality 1 functions that do not meet the physical separation requirements of NSTS 08080–1, Standard 32, must be documented on FMEA/CILs and submitted for program consideration.

(b) Wire harnesses and cables in Criticality 1R functions that do not meet the physical separation requirements of NSTS 08080–1, Standards 4 and 20A, must be documented with a standard program waiver request identifying the areas in the Orbiter and listing the Criticality 1R functions involved in the noncompliance and must be submitted for program consideration.

f. Identical components used for different functions shall be treated separately in the FMEA.

g. The following are used as aids in determining the failure modes and causes of subsystem hardware failures:

1. Generic failure modes and causes

2. Released and controlled component, assembly, and detailed engineering drawings and specifications

3. Training aids, as available; e.g., cross–section drawings, photographs, and exploded assembly drawings (not referred to in the FMEA)

4. Actual hardware, if available

h. Critical item summaries for kits will be included and identified separately.

i. In some cases, NSTS 16007, Shuttle Launch Commit Criteria and Background Document, Permits launching with certain hardware failed, thus reducing the failure tolerance levels to below those required by NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specification. For FMEA/CIL purposes, Launch Commit Criteria (LCC) shall not be used in determining criticality; i.e., it shall be assumed that all hardware, including redundancies, will be operating properly at launch.

3.4.2 Interface Requirements and Groundrules

a. The FMEA will cover analyses of subsystem interfaces (including software interaction) within each element. Any inadvertent, erroneous, or loss of signal/function within the subsystem must be analyzed across the interface to determine ultimate effects on crew/vehicle/mission.

b. FMEAs for mechanical and electrical systems will interface at the mechanical–electrical system connector.

c. Failure modes that could propagate to interfacing elements, subsystems, or experiments will be identified. Effects will be specific enough to determine

overall worst–case resultant effects on crew/vehicle in order to determine functional criticality.

d. When conducting FMEAs/CILs for a particular subsystem, interfacing subsystems providing input will be considered to be operating within their specified tolerances.

e. GFE FMEA/CIL data will be evaluated to assess interface effects on other Space Shuttle element FMEAs and CILs.

3.4.3 Criticality Requirements and Groundrules

a. For design purposes, the criticality categorization for an item shall be made on the basis of worst–case potential failure effect. This includes possible catastrophic effects as well as the effects of loss of hardware functions regardless of probability of occurrence. The criticality categorization for an item whose failure affects the loading or pressure on primary structure, thermal protection system, or pressure vessels, is based on the worst–case potential effect of exceeding the allowable load (the maximum load which the structure can withstand without rupture or collapse). For program operations, the criticality categorization for a failure mode may be made on the basis of credible or realistic failure effects. This will be based on an understanding of the documented characteristics of the certified design and an operational assessment of the failure effects.

b. All identified failure modes will be assigned a functional criticality based on the definition of criticality in Paragraph 3.2.d1. The Space Shuttle Vehicle Engineering Office and EVA and Crew Equipment Office shall also assign a hardware criticality for all identified failure modes (reference Paragraph 3.2.d2).

c. Functional criticality shall be determined by the categorization of the failure mode effect on the subsystem/mission/crew/vehicle, assuming loss of all redundancy (like and/or unlike, operational and/or standby) for performing the function. Figure 3–1 illustrates the analytical logic for criticality determination of all functional hardware failures.

   NOTE: When the Functional Criticality is 1R or 2R, an explanation shall be provided indicating the functional effect of loss of all redundancy. List/identify those redundant functional paths which must be lost before the failure effect would be manifested.

d. Hardware criticality, unique to Space Shuttle Vehicle Engineering Office and EVA and Crew Equipment Office, will be determined by the categorization of the worst–case singular direct effect of the identified failure mode of a hardware

item. In assigning hardware criticality, the availability of redundancy (like and/or unlike, operational and/or standby) is considered (see Figure 3–2).

e. Hardware Criticality 2 failure modes are defined as: (1) single failures which would cause “loss of mission,” or (2) failures where next failure of any redundant item (like or unlike, operational and/or standby) could cause loss of crew/vehicle.

NOTE: “Loss of mission” is defined in Paragraph 3.2m.

f. In determining the worst–case criticality for a unique item/failure mode combination where the item performs a different function depending upon mission phase, the worst–case functional criticality shall be listed. The CIL page should also identify less severe criticalities from other mission phases if other waiverable conditions are known.

EXCEPTION: The requirement to identify less severe criticalities from other mission phases does not apply to the SRB project.

g. In determining classification of criticality categories, it shall be assumed that nominal crew actions will be performed to activate standby redundant items as long as detectability and time to effect requirements of Paragraph 3.4.5a are met. Manual standby redundancy activation must be a premission developed procedure that is nominally trained. Subsequent to the Critical Design Review (CDR), defined and approved in–flight operational controls such as Extravehicular Activity (EVA), In–flight Maintenance (IFM), or contingency provisions or procedures may be considered as risk mitigation, thereby allowing downgrade of the criticality. For a defined and approved operational control to be allowed to downgrade criticality, the documentation of the control should be annotated with reference to the applicable CIL item. Although human error (mishandling during manufacturing, testing, transportation, ground turnaround, and/or crew errors) is not normally addressed when evaluating or presenting hardware failure modes, it should be considered as a cause when a given manufacturing process or assembly procedure is crucial to the operation of the design and is instrumental in contributing to a particular failure mode. This is especially important when the processes or procedures result in causes that cannot be detected in subsequent inspection and test activities.

h. The criticality of emergency system failure modes prior to STS–44 was established on the basis of the failure effect on crew or vehicle, regardless of the number of other subsystem failures which must occur before the use of the emergency system is required. Backup or standby equipment was not considered emergency systems.

New or revised emergency system failure modes identified beginning with STS–44 shall have their criticality established on the basis of the failure effect on crew or vehicle, including the number of other subsystem failures which must occur before the use of the emergency system is required. The least number of failures required to activate the emergency system, plus the least number of failures of the emergency hardware itself, plus the number of crew procedural workarounds that would preclude loss of crew or vehicle should be counted when determining the level of redundancy that exists. If the number of failures total more than three, the items should be classified as Criticality 1R "non–CILs" not requiring retention rationale. (These items do not require waiving.)

1. When assigning criticality to an item whose failure results in use of an emergency system, the emergency system shall be considered as "unlike redundancy" which provides additional protection for a particular failure mode; e.g., a single failure in the Remote Manipulator System (RMS) resulting in the inability to drive any joint which would prevent closure of the payload bay doors would be classified as Functional Criticality 1R since the RMS jettison system provides an unlikely way of allowing closure of the doors.

2. When assigning criticality to an item not in an emergency system, and loss of the emergency system is part of the redundant string of failures, then all failures which cause the activation of the emergency system shall be considered.

i. The criticality assigned to pressure carriers (pressure lines and vessels) reflecting the worst–case failure effect should include potential shrapnel damage to the vehicle/subsystems resulting from rupture of nonfilament–wound tanks, potential overpressurization caused by releasing substantial quantities of fluids from ruptured lines or tanks, or depletion of consumables. The failure of any tank containing a fluid medium which, because of its location in an enclosed compartment, could cause compartment overpressurization leading to structural failure (vehicle loss) will be classified as Criticality 1 for the tank rupture mode. A single failure resulting in leakage of LH_2, H_2, N_2H_4, MMH, N_2O_4, or NH_3 shall be classified as Criticality 1. Leakage of LO_2 or O_2 shall be classified as Criticality 1 when an ignition source could be present.

j. The criticality of instrumentation and test ports shall be assessed according to their function. Where instrumentation (e.g., pressure transducer) penetrates the wall of a component or line and structural failure of the joint would result in

gross leakage, the failure mode shall be considered as a failure of the component or line. The criticality of the instrumentation, therefore, would not be affected in such instances.

k. When worse–case effect of a specific failure mode results in a launch delay, the criticality shall be classified as Criticality 3. Other prelaunch failure modes shall be classified according to their worst–case effect.

l. Software capabilities and features which provide protection, automatic or manually selectable overrides, monitoring switch–over, alternate software modes, etc. shall be considered in assigning criticality.

m. For failure modes resulting in a safe main engine shutdown, hydraulic/pneumatic lockup, or performance degradation, the functional criticality shall be classified as 1R.

n. SSME criticalities shall be determined based upon the following criteria:

   1. Since vehicle thrust is a critical function, the analysis shall be based upon the integrated functional relationship among three engines.

      NOTE: Exception: Per PRCBD S040107V, dated 05/23/90, the SSME project is granted an exception, which revises the above requirement by allowing the SSME criticality analysis to be based upon a single engine.

   2. Hydraulic/pneumatic lockup or erroneous safe main engine shutdown that occurs during the start phase, prior to SRB ignition, shall be classified as Criticality 3.

   3. The failure scenario shall be contained in the disposition and rationale section to explain the failure(s) which result in the assigned criticality.

o. Failure modes of flight hardware (while on the launch pad or during ascent) resulting from lightning shall not be considered for FMEA/CIL purposes. The catenary lightning protection system at the launch pad, in conjunction with launch commit criteria during ascent, make consideration of lightning as an ignition source an extremely low probability of occurrence. Hazards associated with lightning will continue to be documented.

3.4.4 Redundancy Requirements and Groundrules

a. In determining the functional criticality of an item, associated hardware which provides safety features for a particular function may be included as “unlike redundancy” since it provides protection against the effects which would be

manifested if the item it is supplementing fails. For example, the main landing gear pyrotechnic uplock release assembly provides a redundant (though unlike) method of releasing the landing gear if the hydraulic system malfunctions.

b. Redundancy screens must be addressed for all functionally redundant hardware items and determination of "PASS", "FAIL", or "N/A" must be identified for all Functional Criticality 1R and 2R items. For Functional Criticality 1, 2, and 3 items, redundancy screens should be identified as N/A (not applicable).

1. Redundancy Screen A – Redundant hardware item is capable of checkout during normal ground turnaround with no vehicle design modification. Ground turnaround, as defined in the OMRSD, is the time from crew egress to launch.

   NOTE: This screen is not applicable to pyrotechnic devices, excluding electrical control circuitry.

2. Redundancy Screen B – Loss of a redundant hardware item is readily detectable during flight. (For explanation of "readily detectable", see groundrules under Paragraph 3.4.5.)

   NOTE: This screen is not applicable for the following:

   (a) All functionally redundant paths of a subsystem, where only one path is operational at any given time (standby redundancy). Relief valves, applicable switches, and circuit breakers shall be considered as standby redundant items.

   (b) Pyrotechnic devices, excluding electrical circuitry.

   (c) Mechanical linkage.

   (d) Critical items of redundant functional paths which meet one of the following criteria:

      (1) Functional Criticality 1R items which are two fault tolerant or greater and of which at least two remaining paths are readily detectable during flight

      (2) Functional Criticality 2R items which are single fault tolerant or greater and of which at least one remaining path is readily detectable during flight

3. Redundancy Screen C – Loss of all redundant hardware items cannot be the result of a single credible cause, such as contamination. (Fire and explosion are excluded from this screen). As a groundrule, it may be assumed that hardware items will be qualified and properly installed to

withstand the “design–to” environmental conditions. This screen shall be shown as fail when a SFP could result in the loss of redundant functions; i.e., loss of a function receiving power from two independent power sources through redundant wire harnesses connected by a single connector so that failure of the connector would result in loss of the function.

c. For unlike redundant items, which are identified separately in the FMEA, Redundancy Screens A and B shall be applied to each item individually.

d. For SSME critical items designated as Criticality 1R where the first failure results in an intact abort (SFP), the redundancy screens shall be addressed on the redundant hardware.

e. Hardware not meeting design safety factor requirements shall not be considered as “redundancy” when assigning criticality.

3.4.5 Detectability Requirements and Groundrules

a. Failure detectability assumes the capability of a crew member to respond to onboard alerts, realtime monitored displays, or visual indications when the failure of the hardware item only occurs while the crew member is operating and observing the item. Redundancy activated by automatic detection and switchover, shall be considered as passing the in–flight detectability screen (Redundancy Screen B). However, if time for corrective action exceeds time to effect, that failure mode shall be deemed not “readily detectable” and the in–flight detectability screen shall be shown as “FAIL”. Telemetry may be used during Acquisition of Signal (AOS) periods. (If telemetry is the only method of detectability and the system/hardware being analyzed is operating during Loss Of Signal [LOS] periods, the in–flight detectability screen shall be shown as “FAIL” unless sufficient time is available to allow corrective action following the next AOS). Periodically detectable failure modes shall also fail Screen B if, during an undetectable period (i.e., LOS periods, sleep periods, etc.) a subsequent failure would yield a Criticality 1 effect.

b. When operability of a standby redundant item cannot be detected during flight until the redundant item is called upon for use, the item shall be shown as “not applicable” for the “B” screen.

3.4.6 Instrumentation Requirements and Groundrules

a. Instrumentation FMEAs (e.g., sensors and signal conditioners) will be included in the using subsystem FMEA. Criticality 3 instrumentation may be listed on one FMEA form by family or type. FMEAs for (1) Criticalities 1 or 2 and (2) Criticality 1R and 2R instrumentation that fails a redundancy screen or the screen is “N/A” will be individually listed and included in the using subsystem CIL.

b. Instrumentation criticality shall be established by the using subsystem utilizing analysis which includes evaluations of the effects of an instrumentation failure upon or within the subsystem.

c. See criticality groundrule Paragraph 3.4.3j.

3.4.7 Leakage Requirements and Groundrules

a. The external leakage failure mode of any hardware item from any source (except mating of two surfaces by inspectable welding, brazing, or Permaswage) shall be considered a credible event, and the resultant worst–case effects shall be identified.

NOTE: Welds or brazed joints that cannot be inspected shall be analyzed for leakage and for structural failure effects.

b. The internal leakage failure mode of any hardware item shall be considered credible. When internal leakage is a cause resulting in a Criticality 1 or 2 failure mode effect, it shall be noted.

c. Pressure carriers (lines and pressure vessels) shall be classified by worst–case mode, including external leakage. Lines shall be considered separately for each independent medium. Special lines (e.g., mechanical bellows and flex lines, excluding cold plate fittings) shall be identified individually. Tanks shall also be identified individually.

3.4.8 Supplementary Clarification and Groundrules to be Used for Specific Data Elements

a. Item Nomenclature – Identify basic identifying noun, then any modifiers or descriptions; e.g., “valve, solenoid”.

b. Quantity – Identify the total number of items having identical basic part numbers performing the same function in the subsystem.

c. Part Number – Dash numbers to basic part numbers are required when the basic part number has dash numbers having differences in the failure mode and effects.

d. Failure Modes – Identify first the basic failure mode (keyword), then any additional modifiers necessary to fully describe the specific failure mode (the exact manner in which the item fails). Failure mode keyword identifiers should include but not be limited to those listed in Tables 3.7, 3.8, and 3.9.

e. Mission Phase – Indicate which mission phase(s) the specified failure mode effects would be manifested. If the failure occurs at discrete points in time

within a given mission phase, and different effects may be observed, it may be necessary to specify the subphase or event when discussing the effects. Each project element shall define the specific mission phases applicable to the analysis for that element, including beginning and ending points for each mission phase identified.

f. Abort Critical Components – Items whose criticality is increased to 1 (or in the case of Orbiter, redesigns approved after February 1, 1992, which reduce the system redundancy for intact abort operations to less than that provided prior to the redesign [fail safe minimum] and new designs approved after February 1, 1992, which have less redundancy for intact aborts than for normal mission operations) during intact aborts, shall be indicated and explained to describe why the item becomes more critical at that time when discussing the effects.

NOTE: For complete definitions of intact aborts (Return to Launch Site, Abort–to–Orbit, Abort–Once–Around, and Transatlantic Abort Landing), see NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specification.

g. Cause(s) – Causes resulting in the identified failure mode should be listed, and should include but not be limited to those listed in Table 3.10.

h. Effects

1. Specify effect of failure mode on subsystem, interfacing subsystem, mission, crew, and element/vehicle. When “no effect” is applicable, so state.

2. Sufficient explanation shall be provided for abort critical components.

3. When an item fails a redundancy screen, an explanation of why the item fails the screen shall be provided.

4. When a detection system is available but would not allow sufficient time to safely correct the situation, this will be indicated and explained.

i. Time to Effect/Reaction Time – The analysis shall determine the time for the failure effect to occur and will be specified as follows:

Immediate	– less than 1 second
Seconds	– 1 to 60 seconds
Minutes	– 60 seconds to 60 minutes
Hours	– 60 minutes to 24 hours
Days	– 24 hours to mission complete

The descriptor which indicates the shortest credible time or time range available to correct the situation before the effect is manifested shall be identified.

j. Correcting Action – Describe any action, automatic or manual, which is in place to circumvent the specified failure. Also identify any alternate means (utilizing "unlike" hardware) of accomplishing the function performed by the item or its assembly. If none, so indicate. For instruments (sensors, transducers, etc.) that provide measurements assessed as critical to vehicle/crew safety or mission continuation, the FMEA will identify the redundant or alternate measurements by JSC 18206, Shuttle Data Integration Plan, identification number.

k. Operational Use

1. Describe any "special" operational techniques (flight rules, crew procedures, special crew training) which are required to either prevent the particular failure mode from occurring or to mitigate its effect once it has occurred. These special techniques include contingency actions such as EVA and unplanned in–flight maintenance procedures; e.g., Ku–band antenna EVA stowage.

2. Standard operational techniques which can be expected from the crew to initiate designed–in standby (i.e., crew actions assumed to be performed in assigning criticality for the failure mode) are not considered operational use retention rationale.

3. The rationale should include what shall be done to protect against the next failure; e.g., when an MDM fails so that insight into fuel cell delta volts is lost, the main bus of the affected fuel cell must be cross–tied to gain insight into the systems performance should another cell crossover failure occur.

4. It is assumed that any nominal crew training required for these actions will be performed. If any special training is required for safety, this training requirement shall be included; e.g., actions that are required within seconds after the failure has occurred prohibiting the use of a written procedure.

3.4.9 System Level Effects

All hardware analyzed and documented by the FMEA/CIL shall be reviewed "end–to–end" to determine system dependencies such as pneumatics, electrical power, and instrumentation. The review shall ensure that all system dependencies are analyzed and documented in the FMEA/CIL. Analysis of a component whose failure may propagate across an interface shall not end at the interface with other subsystems/systems/elements.

It is the responsibility of each element project to initiate the communication lines necessary to determine effects across element interfaces. Inquiries regarding the

determination of effects across element interfaces should be addressed to the Space Shuttle Systems Integration Office at JSC.

3.4.10 Documentation Flow Requirements for Commonality Hardware Items

a. Information developed by one Center necessary for the preparation of FMEAs and CILs by another Center shall be transmitted to the using Center as the information becomes available; i.e., test reports, certification requirements, mandatory inspection points, updated CIL pages, etc.

b. System level failure reports (commonality hardware) shall be processed in accordance with requirements stipulated in NSTS 08126, Problem Reporting and Corrective Action (PRACA) System Requirements, Paragraph 4.6.

TABLE 3.1

FUNCTIONAL CRITICALITY DEFINITIONS FOR FLIGHT HARDWARE

Criticality	Potential Effect or Failure
1	Single failure which could result in loss of life or vehicle.
1R	Redundant hardware item(s), all of which if failed, could cause loss of life or vehicle.
2	Single failure which could result in loss of mission.
2R	Redundant hardware item(s), all of which if failed, could cause loss of mission.
3	All others.

TABLE 3.2

HARDWARE CRITICALITY DEFINITIONS FOR FLIGHT HARDWARE

Criticality	Potential Effect or Failure
1	Loss of life or vehicle.
2	Loss of mission or next failure of any redundant item could cause loss of life/vehicle.
3	All others.

NOTE: Hardware criticality is applicable to Orbiter and GFE elements only. +

TABLE 3.3 (DELETED)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE 3.4 (DELETED)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE 3.5

CRITICAL LRU/HARDWARE LIST

Project Element: _____

Subsystem: _____

LRU/HARDWARE PART NUMBER/ REFERENCE DESIGNATOR	LRU/HARDWARE PART NAME		QTY (per subsystem)	LRU/ HARDWARE CRITICALITY
FMEA P/N	FMEA PART NAME	FMEA NO.	QTY (per subsystem)	FMEA CRIT*
LRU/HARDWARE P/N 345	LRU/HARDWARE–ABC		3	1
XXXXXXXXX	YYYYYYYYY	FMEA NO. 3	(2)	1
XXXXXXXXX	YYYYYYYYY	FMEA NO. 2	(2)	*1RB
XXXXXXXXX	YYYYYYYYY	FMEA NO. 1	(2)	2
CCCCCCCCC	MMMMMMM	FMEA NO. 1	(4)	*3
CCCCCCCCC	MMMMMMM	FMEA NO. 2	(4)	2RB
OOOOOOOOO	LLLLLLLLL	FMEA NO. 1	(3)	1RABC
OOOOOOOOO	LLLLLLLLL	FMEA NO. 2	(3)	2RA
LRU/HARDWARE P/N 678	LRU/HARDWARE–XYZ		4	*1R
XXXXXXXXX	YYYYYYYYY	FMEA NO. 3	(2)	2RB
XXXXXXXXX	YYYYYYYYY	FMEA NO. 2	(2)	1RA
XXXXXXXXX	YYYYYYYYY	FMEA NO. 1	(2)	*2

*An asterisk preceding the nominal mission criticality number indicates if the item is Criticality 1 (or in the case of Orbiter, redesigns approved after February 1, 1992, which reduce the system redundancy for intact abort operations to less than that provided prior to the redesign [fail safe minimum] and new designs approved after February 1, 1992, which have less redundancy for intact aborts than for normal mission operations) during intact abort. An A, B, or C following the criticality number indicates which, if any, of the redundancy screens the item fails to meet.

TABLE 3.6

DATA ELEMENTS OF CRITICAL ITEMS LIST (CIL) REPORT FOR FLIGHT HARDWARE (INFORMATION REQUIREMENTS 2SR–22)

Number	Contents
1	Introduction and Summary – Concise statement on the objectives and scope of the report.
2	Critical LRU/Hardware List – Provides (by subsystem) a listing of LRU part numbers, reference designator (if appropriate), LRU nomenclature, LRU highest level criticality, lower level part numbers identified by the FMEA and respective nomenclature, failure mode number, quantity of items in the subsystem, and criticality for each FMEA/CIL number, indicating redundancy screen(s) failed as applicable. (See Table 3.5 for data elements and format.)
3	Item Identification – Identification of item for which the FMEA is being conducted including the following: a. System/subsystem/assembly b. Item (component) part number (drawing number by which the contractor identifies and describes each component or module) and name c. LRU part number, name, and quantity (in the subsystem) d. Reference designator (identification of the component or module on the schematic) e. Part number and name f. Quantity – total number of items in the subsystem with the noted function
4	Criticality Category – Identifies the criticality category of each CIL item. The items shall be grouped into criticality categories. NOTE: If items are categorized a Criticality 1R or 2R, effects should list the number of success paths remaining after the first failure and explain how loss of each succeeding path affects the operation of the item to arrive at the resultant effect of loss of all redundancy. a. Rationale for Criticality Category Downgrade – Identifies the original criticality based on design and rationale for criticality downgrade following the CDR due to the consideration of defined and approved operational controls.

TABLE 3.6

DATA ELEMENTS OF CRITICAL ITEMS LIST (CIL) REPORT FOR FLIGHT HARDWARE (INFORMATION REQUIREMENTS 2SR–22) – Continued

Number	Contents
5	Intact Abort Mode Criticality – Include all items not meeting failure tolerance requirements during intact abort.
6	FMEA Reference – Items shall be referenced to the FMEA from which they were derived.
7	Prepared By/Approved – Identifies the analyst preparing the CIL and the appropriate individual responsible for the overall FMEA/CIL effort (Reliability, Design, Management).
8	Date/Superseding – The date on which each page is approved should be entered. If the page being submitted supersedes a previously submitted page, the date of the previous page should be entered on the superseding line. If there has been no previous submission, "None" should be entered.
9	Unique FMEA/CIL Identification Number – A number which uniquely identifies the item/failure mode combination.
10	Function – Concise statement of the function performed by the hardware item being analyzed. NOTE: EXCEPTION: It is not required that this data element be provided in the Critical Items List (CIL) for the SSME and SRB.
11	Failure Mode – Identification of the specific failure mode after considering the four basic failure conditions below: a. Premature operation b. Failure to operate at a prescribed time c. Failure to cease operation at a prescribed time d. Failure during operation
12	Cause(s) – For each applicable failure mode, identify the major cause(s) including operational and environmental stress factors described, if known. NOTE: EXCEPTION: It is not required that this data element be provided in the Critical Items List (CIL) for the SSME.

TABLE 3.6

DATA ELEMENTS OF CRITICAL ITEMS LIST (CIL) REPORT FOR FLIGHT HARDWARE (INFORMATION REQUIREMENTS 2SR–22) – Continued

Number	Contents
13	Failure Effect – Identifies the specific failure mode effects. The effect statement should specify the safety and mission success consequences on the subsystem, interfacing subsystem, mission, crew/vehicle/element.
14	Success Paths Remaining After First Failure – Indicate number of success paths (including unlike redundant items) after first failure until worst–case effects are reached.
15	End Item Effectivity – Nomenclature necessary to identify failure mode with a specific flight configuration; i.e., Orbiter–Vehicle number (OV–102, etc.), External Tank–block numbers, SRBs–DFI block/operational block, and SSME baselined engine configuration with variances.
16	Mission Phases – Phase of mission in which failure occurs. Mission phases shall be defined by each of the project elements.
17	Time to Effect/Reaction Time – The descriptor which indicates the shortest credible time or time range available to correct the situation before the effect is manifested. NOTE: EXCEPTION: It is not required that this data element be provided in the Critical Items List (CIL) for the SSME.
18	Redundancy Screens – Indicates each redundant screen which the redundant item fails, an explanation of why the item fails the screen shall be provided.
19	Rationale for Acceptability – Identifies the rationale or justification for retaining the critical item. Where no rationale or justification is given, corrective action(s) for eliminating the critical item shall be given. Rationale or justification shall incorporate the following information: a. Design – Identify design features which minimize the probability of occurrence of the failure mode and causes.

TABLE 3.6

DATA ELEMENTS OF CRITICAL ITEMS LIST (CIL) REPORT FOR FLIGHT HARDWARE (INFORMATION REQUIREMENTS 2SR–22) – Concluded

Number	Contents
	b. Test – Identify specific tests accomplished to detect failure causes during acceptance test and certification tests. If turnaround checkout testing is accomplished to verify this item, details of test performed are not necessary. The following generic statement, "any turnaround checkout testing is accomplished in accordance with OMRSD" may be used.
	c. Inspection – Note that specific inspection points are included to determine that specific failure modes causes are not inadvertently manufactured into the hardware. Identify inspections which minimize the probability of occurrence of the failure mode and causes.
	d. Failure History – Provide a statement indicating that current data on test failures, flight failures, unexplained anomalies, and other failures experienced during ground processing activity can be found in the PRACA data base.
	e. Operational Use – In general terms describe any special operational techniques (flight rules, crew procedures, special crew training) which are required to either prevent the particular failure mode or to mitigate its effects once it has occurred. Include contingency actions such as EVA and unplanned in–flight maintenance procedures. However, standard crew actions which are expected to initiate designed–in standby redundancy shall not be included. The actual procedure, flight rule, or training sequence identification numbers should not be included.
20	Revision – An identifier should be placed in the revision block opposite each entry that has been changed since the previous submittal.

TABLE 3.7

TYPICAL FAILURE MODES

Erratic Operation

Fails to Remain Open/Closed

Fails Mid–Travel

Fails to Open/Close

Fails Out of Tolerance

Inadvertent Operation

Intermittent Operation

Internal/External Leakage

Physical Binding/Jamming

Restricted Flow

Structural Failure (Rupture)

Premature Operation

Delayed Operation

Erroneous Output

Partial Output

Open (Electrical)

Leakage (Electrical)

Loss of Output

Fails to Switch

Shorted

Fails to Start/Stop

TABLE 3.8

TYPICAL MECHANICAL COMPONENT FAILURE MODES

Component Type	Failure Modes
Pressure Gage	Erroneous high indication Erroneous low indication
Pressure Regulator	Regulates high Regulates low
Filter	Clog Pass contaminants
Remotely operated valves	External leakage Fail open Fail closed Erroneous position indication
Relief valve/burst disc	External leakage Fail to relieve Fail open
Hydraulic/pneumatic actuators	Fail to actuate Actuate prematurely
Check Valve	Fail open Fail closed
Quick Disconnect	Fail to separate Separate prematurely Leak before/after disconnect

TABLE 3.9

TYPICAL ELECTRICAL COMPONENT FAILURE MODES

Component Type	Failure Modes
Temperature/pressure transducer	Erroneous indication
Rectifier	Fail open Fail short Short to ground
Resistor	Fail short Fail open Short to ground
Capacitor	Fail open Fail short Short to ground
Diode (signal)	Fail open Fail short Short to ground
Transformer	Fail open Fail short
Switch	Fail open Fail closed Short to ground
*Relay	Fail open (contacts/coil) Fail closed (contacts)
Transistor	High output Low or no output Reverse polarity
Sensor (discrete)	Erroneous output (high/low) Low or no output

*NOTE: Relays with multiple contacts will require assessment of each contact set for effect.

TABLE 3.9

TYPICAL ELECTRICAL COMPONENT FAILURE MODES – (Continued)

Component Type	Failure Modes
Power supply	High output Low or no output
Amplifier	Low or no output Erroneous output
Electronic modules	Low or no output Erroneous output
Generator	Low or no output High output Erroneous output
Meter	Erroneous indication Fail open Fail short
Diode (zener)	Fail open Fail short
Thermocouple (thermistor)	Fail open Failed closed
Indicator lamp	Fail open Fail short
Light emitting diodes and digital displays	No indication Erroneous indication
Fuse	Premature operation Failure to operate
Motor	Inoperative

TABLE 3.9

TYPICAL ELECTRICAL COMPONENT FAILURE MODES – (Concluded)

Component Type	Failure Modes
Circuit Breaker	Premature trip Fail to trip
Silicon control rectifier	Fail short Fail open
Inductors	Fail short Fail open
Solenoid (Relay)	Fail activated Fail deactivated
Battery	Fail short Fail open

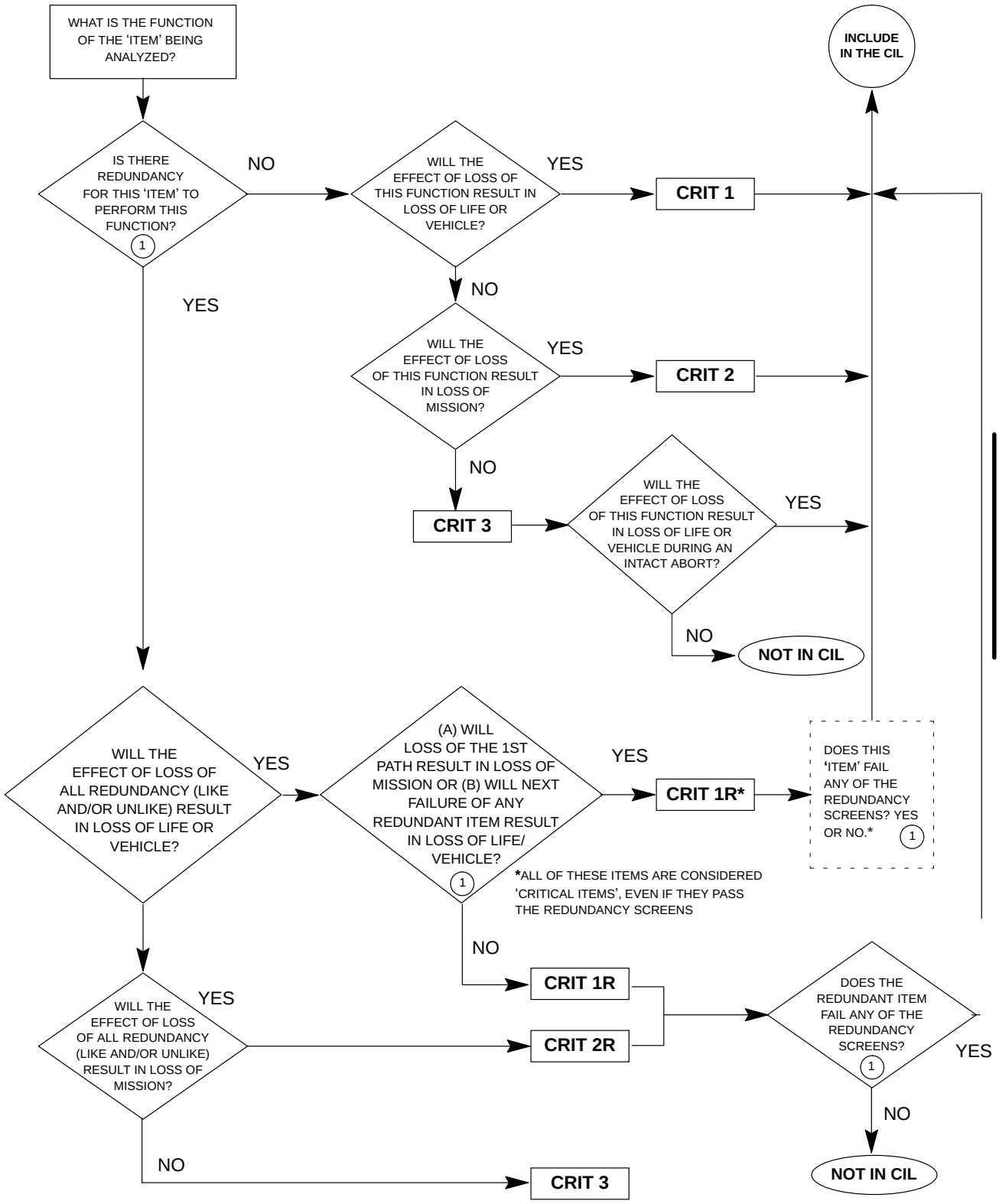
TABLE 3.10

TYPICAL FAILURE MODE CAUSES

Acoustics	Ionizing Radiation	Loss of Input
Contamination	Temperature	Vibration
Erroneous Input	Partial Input	Electromagnetic Fields
Mechanical Shock	Thermal Shock	Piece–Part Structural Failure
Overload	Acceleration	Chemical Reaction
Vacuum	Pressure (High/Low)	

FIGURE 3–1

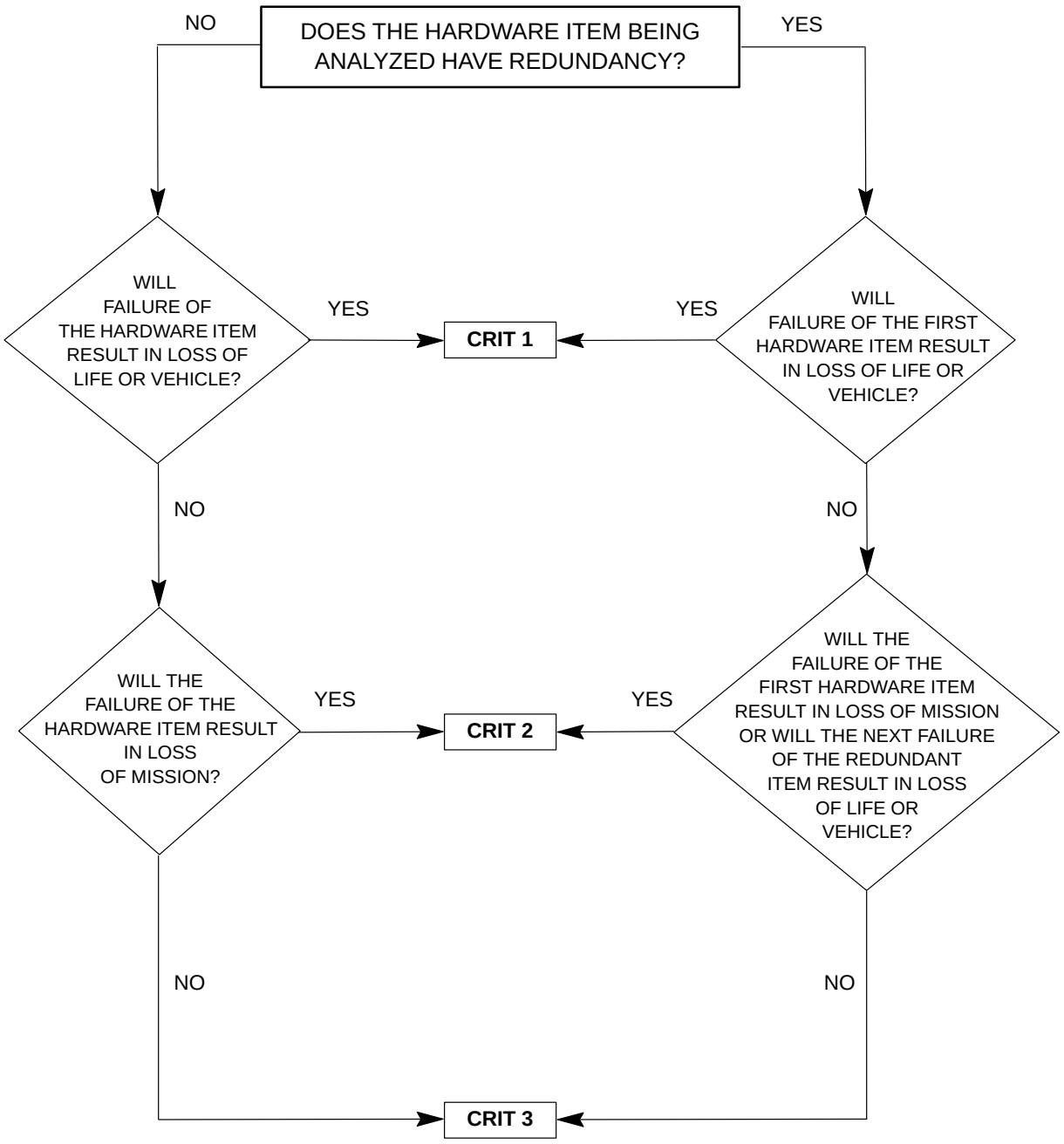
FMEA/CIL SCREENING PROCESS FOR DETERMINING FUNCTIONAL CRITICALITY FOR FLIGHT SYSTEMS



NOTE (1): "ITEM" = HARDWARE ITEM/UNIQUE FAILURE MODE COMBINATION

FIGURE 3–2

FMEA/CIL SCREENING PROCESS FOR DETERMINING HARDWARE CRITICALITY*



* APPLICABLE TO ORBITER SUBSYSTEMS AND GFE ONLY

THIS PAGE INTENTIONALLY LEFT BLANK

4.0 INSTRUCTIONS FOR GROUND SUPPORT EQUIPMENT (GSE) FAILURE MODES AND EFFECTS ANALYSIS AND CRITICAL ITEMS LIST

4.1 SCOPE

This section further defines and implements NHB 5300.4 (1D–2) and provides the requirements and groundrules for performing FMEAs and preparing CILs on critical GSE. NHB 5300.4 (1D–2) allows GSE FMEA and CIL tasks to be combined with the hazard analysis task to preclude duplication of analytical work and documentation. This section applies to the "as–built" configuration GSE used to test, checkout, process, handle, and transport Space Shuttle flight hardware at the launch and landing sites, including such equipment used at other sites that is common to that used at launch and landing sites. FMEAs will be prepared on all critical GSE except for those items excluded due to groundrules contained in Paragraph 4.4.

4.2 GSE DEFINITIONS

These definitions are vital to an understanding and interpretation of the requirements and groundrules contained in this section and shall be used as the reference source for GSE FMEA and CIL terminology.

a. Component – A combination of parts, devices, and structures, usually self contained, which perform a distinctive function in the operation of the overall equipment. A "black box" (e.g., transmitter, power supply, cryogenic pump, filter assembly).

b. Correcting Action – An identification of actions, automatic or manual, which could be taken to mitigate the effect of failure.

c. Critical Item – A critical item is defined as any one of the following:

   1. A Criticality Category 1, 1S or 2 Single Failure Point.

   2. A redundant hardware item where the second failure results in loss of life or vehicle and the item is not capable of checkout during normal ground operations (i.e., a single fault tolerant item which fails Redundancy Screen A.)

d. Critical System – A system is assessed as critical if loss of overall system function or improper performance of a system function could result in loss of life, loss of vehicle, or damage to a vehicle system.

e. Criticality – The relative measure of the consequences of a failure mode. (See Table 4.1 GSE Criticality Category Definitions.)

f. Criticality Assessment – An analysis of each system function to determine if loss or improper performance of the function could result in loss of life and/or vehicle or damage to a vehicle system.

g. Fail Safe – The ability to sustain a failure without causing loss of life/vehicle or damage to a vehicle system. (Includes the capability to safe the systems and successfully terminate operations.)

h. Failure – The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

i. Failure Mode – A description of the manner in which an item can fail.

j. Function – The activity or operation that a part, component, or system must perform to accomplish its intended purpose.

k. Interface – The point or area where a relationship exists between two or more parts, systems, programs, persons, or procedures wherein physical and/or functional compatibility is required.

l. Loss of Vehicle System – Loss of the capability to provide the level of system performance required for normal or emergency operations.

m. Line Replaceable Unit (LRU) – An item whose replacement constitutes the optimum organizational maintenance repair action for a higher indenture item, i.e., any assembly which can be removed and replaced as a unit from the system at the operating location.

n. Passive Component – A component that may be necessary to the performance or structural integrity of the system but has no active function.

o. Prerequisite Control Logic – GSE software program logic that assures proper sequence of commands.

p. Reactive Control Logic – GSE software program logic that assures automatic reaction to indicated failures.

q. Redundancy – Multiple ways of performing a function.

    1. Operational Redundancy – Redundant elements, all of which are fully energized during the subsystem operating cycle. Operational redundancy includes load sharing redundancy wherein redundant elements are connected in such a manner that, upon failure of one unit, the remaining redundant elements will continue to perform the subsystem function. Switching out the failed element is not required.

2. Standby Redundancy – Redundant hardware items that are nonoperative until they are switched into the subsystem upon failure of the primary items. Switching can be accomplished by either automatic or manual means.

3. Like Redundancy – Identical hardware items performing the same function.

4. Unlike Redundancy – Nonidentical hardware items performing the same function. Safety features which provide protection for specific failure modes are considered as unlike redundancy for that failure mode; i.e., relief valves which provide protection against overpressurization after failure of a regulator.

r. Safety or Hazard Monitoring System – A system whose function is to detect or combat a hazardous situation which has occurred because of prior failures or events during hazardous operations.

s. Single Failure Point (SFP) – A single item of hardware, the failure of which could result in loss of life/vehicle or damage to a vehicle system.

t. Waiver – A written authorization, granted after the fact, for use or acceptance of an article which does not meet the specified requirements.

u. 1R Non–CILs – Functional Criticality 1R failure modes which exceed the NSTS 07700, Volume X, fail–safe requirement by being at least two–fault tolerant, and satisfy the NSTS 07700, Volume X, requirements for redundancy verification and separation of critical functions (i.e., pass redundancy screens).

4.3 FAILURE MODES AND EFFECTS ANALYSIS AND CRITICAL ITEMS LIST REPORT CONTENT

4.3.1 Failure Modes and Effects Analysis

Each element or prime contractor shall perform a FMEA and the resulting worksheets and supporting data (block diagrams, schematics, etc.) shall be retained by the element project.

4.3.2 1R Non–CILs

1R non–CIL information shall be included in the CIL. The information contained in this grouping shall meet the criteria of Paragraph 4.3.3a and c and, as a minimum, contain data elements 1 through 7 as defined in Table 4.3 (rationale for acceptability is not required for 1R non–CIL items).

4.3.3 CIL Content

The CIL contains the Critical Hardware List (CHL) and the individual CIL sheets. The CIL contains the following information:

a. Critical LRU/Hardware List – Provides (by subsystem) a listing of LRU part numbers, reference designator (if appropriate), LRU nomenclature, LRU highest level criticality, lower level part numbers identified by the FMEA and respective nomenclature, failure mode number, quantity of items in the subsystem, and criticality for each FMEA/CIL number (see Table 3.5 for data elements and format). The Critical LRU/Hardware List will include all critical items.

b. CIL Sheet Acceptance Rationale – Identifies the rationale or justification for retaining critical items and is comprised of the following by data elements:

   1. Design
   2. Test
   3. Inspection
   4. Failure History
   5. Operational Use

c. Analysis Results – This section contains the individual CIL pages describing actual analysis results. The CIL is comprised of items meeting the definition of a critical item contained in Paragraph 4.2c. The CIL pages shall as a minimum contain data elements defined in Table 4.3.

4.3.4 Schedule

The schedule for submittal of CILs and 1R non–CILs will be in accordance with NASA approved 1Rs (see NSTS 07700, Volume V, Information Management Requirements, 2SR–22).

4.4 GROUND SUPPORT EQUIPMENT ANALYSIS REQUIREMENTS AND GROUNDRULES

4.4.1 Preparation Scope and General Requirements

A FMEA shall be performed on critical Ground Support Systems (GSS) in accordance with the following groundrules:

a. General:

   1. Prior to conducting the FMEA, an initial criticality assessment shall be performed to assess each system function and determine if loss or improper performance of the function could result in loss of life and/or vehicle or damage to a vehicle system. This assessment is performed without regard to available redundancy. System functions shall be identified as either critical or non–critical and no criticality category numbers shall be assigned. The criticality assessment shall contain the data elements required by Table 4.4.

2. FMEAs will be performed to the lowest level necessary to identify critical functions and items. For design purposes, the criticality categorization for an item shall be made on the basis of worst–case potential failure effect. For program operations, the criticality categorization for a failure mode may be reassessed for credibility and reasonableness on the basis of operational experience with the equipment. This will be based on an understanding of the documented characteristics of the certified design and an operational assessment of the failure effects. The FMEA is a Single Failure Point analysis and does not address multiple failures with the following clarification:

   (a) The combined effect of failure of two like and/or unlike redundant items which could result in loss of life/vehicle will be evaluated.

   (b) Single failure modes in safety and hazard monitoring systems are evaluated (Criticality 1S). These failure modes assume the hazardous condition being monitored or combatted has already occurred. The combined effect of failure of two like and/or unlike redundant items which could result in loss of the function of a safety or hazard monitoring system will be evaluated for such systems associated with emergency egress of the flight crew. The systems are listed in Table 4.5.

THIS PAGE INTENTIONALLY LEFT BLANK

(c) Failures of redundant items which meet the criteria described in 2(a) or 2(b) above shall be classified as Criticality Category 1R. Requirements for periodic test, inspection or functional validation of these items shall be invoked through the appropriate operation and maintenance requirements documentation. Single failure within the system controls which could cause loss of a 1R item shall not be identified as 1R but shall be listed as a cause of the failure of the 1R items which it controls. Such system controls shall be included in the periodic test, inspection or functional validation requirement invoked on the 1R item.

3. Redundancy screens must be addressed for all Criticality Category 1R items. Determination of “Pass”, “Fail”, or “N/A” (not applicable) must be documented in the summary list of 1R items. The GSE redundancy screens are defined as follows:

   (a) Screen A – The redundant item is capable of being checked and verified during normal ground operations.

   (b) Screen B – Loss of the redundant item is readily detectable by the ground crew. (This screen is not applicable to standby redundancy.)

   (c) Screen C – Loss of all redundant items cannot result from a single credible cause, such as contamination.

4. Electrical power, pneumatics and controls to non–critical functions shall be considered non–critical. If a function is critical, then the electrical power, pneumatics and controls to that function shall also be considered critical and analyzed in the FMEA.

5. Electrical power and pneumatic system support for redundant components shall be analyzed to assure that the primary and secondary legs are fed by different sources (no single failure can affect operation of both). System controls shall be analyzed to assure that primary and secondary controls are on independent data buses and no single failure can affect operation of both.

6. Structural or passive components will be listed but will not be analyzed in the FMEA except for the items in Paragraph 4.5.1 and Paragraph 4.5.2.

7. Failures due to human error in system setup (e.g., manual valves erroneously in the wrong position) shall not be considered in the FMEA. Such items that constitute a safety concern shall be considered in the Hazard Analysis.

8. Hypergol emergency exhaust fans shall be analyzed to assure that appropriate controls are provided so that these systems cannot be inadvertently activated by a single failure.

9. Criticality 1S shall be used in assessing components in safety systems (e.g., fire detection and fire suppression).

10. Safety devices (e.g., relief valves, circuit breakers) shall be categorized in accordance with their failure effect on the system, flight hardware, or personnel safety and will not be categorized 1S unless in a safety system and failure will cause loss of a safety system function (i.e., a circuit breaker in the 60–Hz power system whose failure in the premature trip mode interrupts power to a safety system).

11. Failure of equipment provided to detect non–hazardous contamination shall be considered Criticality 3.

12. Elevators provided for emergency egress of the flight crew will require a FMEA.

13. Hoists/winches utilized to raise/lower platforms that can impact the vehicle during raising/lowering operations shall require a FMEA.

14. Air conditioning/humidity control systems shall require a FMEA only where flight systems and launch related equipment are dependent on humidity and/or cooling. Air conditioning used for hazard proofing by pressurization shall require a FMEA.

15. Fire extinguishing and fire suppression systems, including water deluge, ansul, and halon, shall require a FMEA when failure to operate or inadvertent operation could cause:

    (a) Loss of flight or ground crew

    (b) Damage to flight hardware

    (c) Loss of a critical function

16. Fire alarm systems shall not require a FMEA unless a review of vendor data or design data shows they do not meet National Fire Protection Association (NFPA) requirements.

17. FMEAs shall be required on ground computer hardware (e.g., LPS) used to command and control flight hardware to the level necessary to identify critical effects.

b. Electrical:

1. The FMEA shall be performed on electrical/electronic equipment to the “black box” level. All Criticality 1 and 2 failure effects will require analysis within the “black box” to the level necessary to identify causes of the critical failure mode.

2. FMEAs on wire harnesses, cables, and electrical connectors shall not be required except where a single failure (short or open circuit) could result in loss of life or vehicle or where system design requirements of NSTS 08080–1, Space Shuttle Manned Spacecraft Criteria and Standards, (Standard 4B and Criticality 1S applicable to Standard 20A) for physical separation of redundant critical functions in harnesses and connectors are not met and could result in loss of crew/vehicle, due to a single failure.

3. Fire alarms and area warning systems shall be considered to provide backup capability to each other and shall be evaluated to determine if they are dependent on the same source of power.

4. Hardwire safing shall be considered as an integral part of the system for which it was provided to safe.

c. Fluids:

1. Internal leakage shall be included in the assessment of the “fail open” failure mode.

2. External leakage shall be considered where leaks are detrimental to system operation or personnel safety.

3. All components located in the system downstream of the final filter shall be assessed for a possible source of contamination (e.g., transducers, temperature probes, component softgoods).

4. Filters, orifices and flex hoses will be analyzed in the FMEA of the using system and comply with Paragraph 4.5.2.

4.5 SPECIAL FMEA PROCEDURES

Because of the complexity of GSE design and operations, some special groundrules/ procedures shall be applied in the performance of the FMEA in the situations specified below.

4.5.1 Failure Modes and Effects Analysis of Cranes/Hoists

The following approach shall be used in analyzing the mechanical drive system for cranes/hoists:

a. Diagrams showing the relationships between each component shall be developed for the mechanical drive system, commencing with the hook and working back through the drive train.

b. The analysis shall assess all active components between the load hook and the nearest brake since failure of these components could result in dropping the load. The following groundrules shall be used:

    1. If the hoist has only one brake, the brake shall be identified as a Single Failure Point and the criticality shall be assigned based on the worst–case effect of its failure. An eddy current brake shall not be considered capable of holding the load.

    2. For shafts located between the drum and brake, the method of shaft attachment shall be analyzed. If the shaft is welded or physically attached to the drum by a method approved by hoisting standards, then the shaft attach points shall be considered passive.

    3. Bearings on drums and shafts shall be analyzed only to determine if the bearings can fail and drop the load.

    4. Gear boxes, speed reducers, and couplings shall be considered Single Failure Points if they are located between the drum and nearest brake.

c. To determine the acceptability of mechanical SFPs identified in the analysis, each potential SFP shall be addressed in accordance with the following:

    1. Does it conform to ANSI and OSHA standards?

    2. Does it have a 5–to–1 design safety margin?

    3. How is it attached or secured to the drive train? Is it attached by approved methods, e.g., are gears captured to the shafts by keys and pressfits or are they integral to the shaft?

d. Redundant items with control circuitry must be analyzed to determine if a single credible failure can affect the controls for both redundant components.

e. A single limit switch on the trolley or bridge drive shall not be identified as a SFP if there is also an acceptable mechanical stop.

f. Non–compliance to the requirements of NSS/G0–1740.9, NASA Safety Standard for Lifting Devices and Equipment, shall be identified in the FMEA.

g. Passive components will not be analyzed in the FMEA. The current list of passive components includes the hook, load block, wire rope, sheaves, and rope

drum. However, the drum shafts shall be analyzed as to the attachment method.

h. The electrical/electronics, valves, pneumatic portion, as applicable, shall be analyzed in accordance with the FMEA requirements and groundrules of Paragraph 4.4.

4.5.2 Analysis of Flex Hoses, Orifices and Filters

FMEAs on flexible hoses, orifices, and filters whose failure could result in loss of life/vehicle or damage to vehicle systems will contain the following information as appropriate:

a. System/subsystem/program model number

b. Drawing number/sheet number/find number

c. NASA part number

d. Manufacturer/name/part number

e. Material

f. Fluid media

g. Diameter/nominal size

h. Maximum allowed working pressure (psig)

i. Proof pressure (psig)

j. Design burst pressure (psig)

k. Element collapse pressure

l. Alignment tolerances/bend radius (flex hose)

m. Failure Effect

n. Critical or non–critical classification and Criticalities 1, 1S, or 2 and 1R will be provided.

o. OMRSD requirements for critical flex hoses, orifices, and filters, such as periodic inspections, scheduled maintenance, proof tests, etc.

4.5.3 Analysis of Computer System Interfaces, Hardware Interface Modules (HIMs) and Power Buses

These analyses are required to determine if any critical or redundant functions would be lost because of failure of a computer interface, HIM or power bus. Inadvertent commands or signals, or lack of required signals, will be analyzed. In the normal process of

conducting the FMEA, each component is analyzed; however, it is often not possible at that time to fully assess the total impact of loss of a computer system interface, HIM/ data link, or power bus because of the multiplicity of functions pertaining to each. It is also possible that computer system interfaces, HIMs/data links, and power buses support different systems designed by different organizations/contractors. It may be necessary to list all functions carried by each computer system interface, HIM, or power bus to determine the effect of loss. The purpose of this analysis is to assure proper division of functions/loads. The following rules shall apply:

a. Critical redundant or backup functions will be evaluated to determine if they are controlled from different HIMs that utilize independent Launch Processing System (LPS) data links. This is necessary since each HIM/data link combination contains approximately seventy–five (75) Line Replaceable Units (LRUs) that could fail and cause loss of HIM control. The goal is ultimately to be able to continue operations through the redundant/backup HIM/data link if a HIM/ data link should fail.

b. The analysis shall consider all possible combinations of HIM card and channel failure, both on and off.

c. Critical redundant or backup functions will be evaluated to determine if they are powered through different circuit breakers by independent power buses.

d. Since there are failure modes that could cause loss of an LPS set, systems that are dependent upon LPS to perform critical functions shall be evaluated to determine if they have hardwire safing panels in addition to any redundant HIMs/data links.

4.5.4 Analysis of Prerequisite and Reactive Control Logic, Launch Commit Criteria (LCC), and Ground Launch Sequencer (GLS)

After the mechanical and electrical design is defined and the basic FMEA is performed, it is necessary to review the software to assure that reliability and safety are not compromised in the implementation of the software system. During the performance of the FMEA, assumptions that were made concerning detectability and utilization of redundancy or backup capability shall require further validation and analysis. The following criteria will be applied:

a. If a manual means of intervention is provided, is there adequate warning and is time available to utilize the capability provided?

b. If an automatic means of intervention is provided, is the reactive control logic adequate to perform the required intervention in adequate time?

c. Where critical sequences or prerequisites must be maintained, does the prerequisite control logic preserve the order of operation?

d. Has the software utilized the mechanical, electrical and data transmission capabilities to the maximum extent? Does the software fully utilize the design features provided (i.e., redundant data/control links)?

e. Can a single erroneous measurement (or failure) in the measurement system allow the count to continue with a failed system?

4.5.5 Analysis of Systems with Hardwire Safing Control

Systems with hardwire safing shall be analyzed using the following criteria:

a. Determine if the electrical power for the safing circuits is fully independent.

b. Analyze hardwire safing circuitry as a part of the operating system (i.e., LOX, LH_2).

c. Evaluate adequacy of hardwire circuits functionally assuming total loss of system control by HIMs/LPS data bus(es).

   1. Assume no control or measurement information is available from CCMS.

   2. Verify the means of detection of potential failures identified in the FMEA that would require use of hardwire safing.

4.5.6 Analysis of Umbilicals, Service Arms and Masts

After analysis of umbilicals, service arms, and masts utilizing the basic FMEA groundrules and requirements, the following analysis will be performed for the inadvertent disconnect failure mode even if no SFPs have been identified:

a. List all functions that would be lost if the unit should inadvertently become disconnected.

b. Determine if loss of any of the functions, singularly or in combination, constitute a Criticality 1, 1R, 1S or 2 effect.

   1. Cryogenic fill/drain and vent in the same umbilical may constitute a Criticality 1 effect.

   2. Electrical power and flammable fluid media could result in a Criticality 1 or 2 effect if both are active at the time of disconnect.

   3. Loss of primary and backup functions could constitute a Criticality 1 effect.

4.5.7 Analysis of Operational Controls

Subsequent to the CDR, defined and approved ground operations procedures, including contingency provisions and operator intervention, may be considered as risk mitigation, thereby allowing downgrade of the criticality of a failure mode. For a defined and approved operational control to be allowed to downgrade a failure mode criticality category, the documentation of the control shall be annotated with reference to the applicable FMEA/CIL documentation.

4.6 END–TO–END FMEA

All equipment required to perform a system function (including system dependencies such as pneumatics and electrical power) will be reviewed end–to–end and included in the FMEA. This review will ensure that all system dependencies are analyzed in the FMEA being prepared or are analyzed in another referenced FMEA. The end–to–end FMEA will evaluate the system as it is configured for operation including flight or ground components that are the design responsibility of other organizations, contractors, or design centers.

TABLE 4.1

GSE CRITICALITY CATEGORY DEFINITIONS

Criticality	Potential Effect or Failure
1	Single failure which could result in loss of life or vehicle.
1R	Two redundant hardware items, which if both failed, could result in loss of life or vehicle (or loss of a safety or hazard monitoring system listed in Table 4.5).
1S	Single failure in a safety or hazard monitoring system that could cause the system to fail to detect, combat, or operate when needed during the existence of a hazardous condition and could result in loss of life or vehicle.
2	Single failure which could result in loss (damage) of a vehicle system.
3	All others.

TABLE 4.2 (DELETED)

TABLE 4.3

DATA ELEMENTS OF CRITICAL ITEMS LIST (CIL) (2SR–22)

Number	Contents
1	Item Identification – Identification of the critical item including the following: a. Item (component) name and find number. b. System/Area. c. NASA and/or manufacturer's part number and manufacturer's name. d. Program model number. e. Drawing/sheet number.
2	Criticality Category – Identification of the criticality category of the critical item.
3	Function – A concise statement of the function performed by the critical item.
4	Failure Mode – Identification of the critical failure mode(s) of the critical item.
5	Cause(s) – Identification of the major cause(s) of the critical failure mode(s).
6	Failure Mode Number – A number which uniquely identifies the item/failure mode combination which can be traced back to the FMEA.
7	Failure Effect – Identification of the specific failure mode effects. The complete scenario leading to the critical effects should be described. A description of the shortest credible time between failure occurrence and manifestation of the critical effect (time to effect) should be included. If failure of the item is not readily detectable, it should be stated here.

TABLE 4.3

DATA ELEMENTS OF GSE CRITICAL ITEMS LIST (CIL) (2SR–22) – Concluded

Number	Contents
8	Rationale for Acceptability – Identification of the rationale or justification for retaining the critical item. Available failure detection methods identified in the FMEA shall be included in one of the following justification paragraphs as appropriate. Where rationale or justification for acceptance of the risk is not adequate, recommendations for corrective action to eliminate the critical item shall be given. Rationale for acceptance shall include the following information: a. Design – Identification of design features which minimize the probability of occurrence of the critical failure mode and causes. b. Test – Identify specific tests accomplished to detect failure mode and causes during acceptance test and certification tests. If turnaround checkout testing to verify the critical item is accomplished via the OMRSD, details of the test are not required and the following generic statement may be used: "Any turnaround checkout testing is accomplished in accordance with OMRSD". If turnaround checkout testing is accomplished via Operational and Maintenance Instructions (OMIs), include details of the test, frequency and OMI number. c. Inspection – Identification of the periodic, pre–operational and post–operational inspections performed to determine whether or not critical failure modes have occurred. Identify inspections which minimize the probability of occurrence of the failure mode and causes. d. Failure History – Provide a statement indicating that current data on test failures, unexplained anomalies and other failures experienced during ground processing activity can be found in the PRACA data base. e. Operational Use – Identification of the corrective action available to mitigate the effects of the failure once it has occurred. The time required to take the corrective action (timeframe) should be included.
9	Rationale for Criticality Category Downgrade – Identifies the original criticality based on design and rationale for criticality category downgrade following the CDR due to the consideration of defined and approved ground operational controls.

TABLE 4.4

DATA ELEMENTS OF CRITICALITY ASSESSMENT

Number	Contents
1	Output – Describe each output commodity and quantity (e.g., 150 psig GN_2, LOX Fast Fill, 28VDC).
2	Function – Provide a concise statement of the function of the output.
3	Time Period – Describe the time frame applicable to the function being assessed. Note that the effect of loss of function may be dependent on a specific time period (e.g., cryo loading, hazardous operations, terminal count sequence).
4	Effect of Loss/Failure – Provide a unique loss statement for each output/ function. Consider failure to operate on time, failure to cease operation on time, failure during operation and premature operation.
5	Criticality – Assess each function as critical or non–critical. A system is assessed as critical if loss of a function or improper operation of a function could cause a Criticality 1, 1S, 1R or 2 effect.

TABLE 4.5

SAFETY AND HAZARD MONITORING SYSTEMS REQUIRING ANALYSIS IN ACCORDANCE WITH GROUNDRULE 4.4.1a.2

Halon Fire Suppression System, Pad A & B

Halon Fire Suppression System, MLP 1, 2 & 3

Dry Chemical Fire Suppression System, Pad A & B

Dry Chemical Fire Suppression System, MLP 1, 2 & 3

Firex Water System, Pad A & B

Orbiter Access Arm, Pad A & B

Slidewire Emergency Egress System, Pad A & B

Emergency Egress Flame Detection System, Pad A & B

Hazardous Gas Detection System, Pad A & B

Hydrogen Leak Detector System, Pad A & B

Hydrogen Fire Detector System, Pad A & B

5.0 CRITICAL ITEMS LIST WAIVER PROCESSING REQUIREMENTS

5.1 WAIVER REQUIREMENTS

NSTS 07700, Volume IV, Configuration Management Requirements, Page iii, states that “All elements of the SSP must adhere to these baselined requirements. When it is considered by the Space Shuttle Program element/project managers to be in the best interest of the SSP to change, waive or deviate from these requirements, an SSP Change Request (CR) shall be submitted to the Program Requirements Control Board (PRCB) Secretary. The CR must include a complete description of the change, waiver or deviation and the rationale to justify its consideration. All such requests will be processed in accordance with NSTS 07700, Volume IV, and dispositioned by the Director, Space Shuttle Operations, on a Space Shuttle PRCB Directive (PRCBD).”

The CIL represents an analysis of the hardware design, highlighting those items which do not meet reliability program requirements contained in NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specification.

5.2 WAIVER SUBMITTALS

CIL waivers document the identification of program risk and its acceptability based on a prescribed set of rationale. Waivers shall be submitted for all CILs meeting the criteria of Paragraph 5.3.

5.2.1 Waiver Submittal Schedule

CIL waivers and waiver updates shall be submitted in accordance with NSTS 07700, Volume V, IR 2SR–22.

If there is adequate time for submittal preparation, then updates required to reflect an increase in baselined risk are to be submitted on a Space Shuttle Program (SSP) CR to the SSP Management Integration Office 30 days prior to the Flight Readiness Review (FRR) to allow review by the System Safety Review Panel (SSRP) and subsequent presentations to the Space Shuttle PRCB, as deemed necessary, by the SSRP. For those mission–by–mission safety assessment items which do not have adequate time for a CIL update, a limited flight effectivity waiver may be granted to NSTS 07700, Volume V, IR 2SR–22 without all the required documentation. This waiver request shall be presented to the SSRP for review and forwarded to the Space Shuttle PRCB for approval. A subsequent CR, containing appropriate program documentation and requesting formal program approval for additional flight effectivities, shall be processed through the PRCB if waiver effectivity was limited. Single mission effectivity items do not require CIL or CIL waiver updates.

The NSTS 07700, Volume V waiver CR shall be accompanied by a Safety Issue Briefing which shall include as a minimum:

a. Description of the issue

b. CILs impacted (number and title)

c. Description of impact to CIL

   1. Failure modes and causes

   2. Criticality and redundancy screen failures

   3. Retention rationale

d. Recommendations on CIL updates and associated schedules

The SSRP will recommend presenting the waiver CR and Safety Issue Briefing to the PRCB when the new CIL or increase in risk topic has not previously been briefed to the SSP Manager through a Special PRCB, PRCB, FRR or Program Mission Management Team (PMMT).

5.2.2 CIL Waiver Information

All CIL baseline waivers or waiver changes which result in increased risk shall require submittal of a CR which includes a waiver matrix (see Figure 5-1) and the rationale for justification of the waiver. The waiver matrix is used in the updating of NSTS 08399, Space Shuttle Program (SSP) Critical Items List (CIL) in WebPCASS. The list of waived items should clearly indicate “change to” information as well as changes, additions or deletions to the matrix. Waiver matrix data elements should include the following as a minimum:

CIL number

CIL date

Waiver code

Effectivity

Criticality

5.2.3 Waiver Codes

See Figure 5–2 for a description of the waiver codes used in the preparation of CIL waiver matrices.

5.3 WAIVER PROCESSING

CIL waiver information will be submitted by CR to obtain program approval of the increased risk. A change shall be considered to involve an increase in risk if any of the following is true.

a. The change introduces a new CIL, failure mode, or failure cause.

b. The change upgrades the CIL criticality or adds additional redundancy screen failures.

c. The change eliminates or adversely affects previously defined CIL retention rationale.

d. The change reduces a margin of safety, even if the change still satisfies factor of safety requirements.

5.3.1 CIL Waivers Requiring Presentation to the PRCB

Not all waivers require presentation to the PRCB. CIL waivers which require presentation include the following criteria, as a minimum (see Figure 5–4):

a. Items directed by the PRCB for resubmittal and presentation

b. New Criticality 1 failure modes

c. New CILs unless they meet criteria for items having generic retention rationale

d. Revised CILs not having generic retention rationale that meet the following criteria:

   1. Criticality upgrades

   2. Additional redundancy screen failures

   3. Items having significant changes to design rationale or changes which result in increased program risk. (This does not include updates to inspections, failure history, test or operational use.)

5.3.2 Other Procedures Used in the Processing of CIL Changes

a. CIL changes which do not result in increased risk may be processed as routine updates. Routine CIL updates shall be submitted in accordance with NSTS 07700, Volume V, IR, 2SR–22 and include a description of change, a listing of CILs included in the package, the project or program element tracking number and the submittal date. NASA element project Safety, Reliability and Quality Assurance shall be responsible for providing surveillance to assure that routine updates do not increase the risk level (reference Paragraph 5.3) of the baselined CILs.

   CIL changes that result in a downgrade of criticality shall be presented to the SSRP to ensure that the risk downgrade rationale is appropriate and that all

element–to–element interfaces have been considered. CILs that are eliminated as a result of hardware being excessed or no longer used do not require review and approval by the SSRP.

b. Changes to operational use statements. For flight hardware, Mission Operations Directorate (MOD) personnel are responsible for the control and maintenance of a data base which correlates CILs with applicable flight rules/ crew procedures.

1. The data base shall be baselined by the PRCB.

2. When changing a flight rule/crew procedure which affects operations performed after failure of a critical item, the change shall be presented to the PRCB.

5.4 PRESENTATION GUIDELINES

CIL waivers requiring presentation to the PRCB shall use the following guidelines:

a. Presentation format optional.

b. Provide drawings, schematics and block diagrams as required to describe the subsystem or hardware which contains the critical items being presented for waiver.

1. Hardware function/purpose

2. Hardware/subsystem operation – applicable mission phases

c. Critical items presentation summary.

1. To be presented:

(a) All applicable critical items requiring waiver except for items defined in c.2 below

(b) All SSME critical items where first failure results in an intact abort, including SSME, SRB, and Orbiter

2. Not to be presented:

(a) Information only items

(b) Items meeting special “preapproved” baselined generic retention rationale (see Figure 5–4)

d. Provide copy of each CIL page.

NOTE: Multiple items can be grouped for presentation provided it is feasible to do so. For example, if a subsystem has multiple heaters and all their

failure modes are the same, the failure effects and retention rationale would be the same; therefore, the items could be presented as a group rather than individually.

e. Summarize key data elements from CIL:

   1. Part name

   2. FMEA/CIL number

   3. Failure mode/cause/effect

   4. Detectability

      (a) Ground checkout

      (b) In–flight

   5. Others as required

f. Emphasize the following data elements of retention rationale:

   1. Design rationale (safety factors, margins, material, etc.)

   2. Test rationale (qualification, acceptance test procedures, OMRSD tests, etc.)

   3. OMRSD Requirements. Identify ground turnaround checkout tests or inspections performed to assure the failure mode for the item being analyzed does not exist, and indicate checkout frequency (every flight, every five flights, etc.)

   4. Inspection requirements (manufacturing inspections, and/or GSE ground turnaround inspections)

   5. Failure History. Provide a summary of failure history for the hardware/failure mode indicating number of failures, when they occurred, causes, corrective action, etc. If hardware has been redesigned so that the failure is no longer applicable, it should not be listed. However, if similar failures have occurred subsequent to the redesign, the previous failure history and the recent history should be included. Failure history shall include acceptance test failures, and unexplained anomalies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE 5.1 (DELETED)

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE 5–1

EXAMPLE OF SSP WAIVER MATRIX

PCIN 40200	SPACE SHUTTLE PROGRAM DOCUMENT CONTINUATION SHEET	PAGE 1 OF X
CR NUMBER XXXXXXX		OFFICE: MV/Space Shuttle Vehicle Engineering Office

DOCUMENT: Critical Items List (CIL) Waivers – Orbiter/Auxiliary Power Unit — Date

WAIVER CODES	CIL NUMBERS	CIL DATE	CRITICALITY	EFFECTIVITY
CHANGE TO:				
1	04–2–TH11–11	XX/XX/XX	1/1	STS–31 THRU STS–999
DELETE THE FOLLOWING:				
3	05–6EH–56000–4	XX/XX/XX	1R/2	STS–26 & SUBS
ADD THE FOLLOWING:				
2	05–6EH–56013–2	XX/XX/XX	1RB/3	STS–29 THRU STS–99 (EXCEPT STS–29)
2	05–6EH–56056–2	XX/XX/XX	1RB/3	STS–28 THRU STS–99 (EXCEPT STS–29)
2	05–6EH–56009–2	XX/XX/XX	1RB/3	STS–28 THRU STS–99 (EXCEPT STS–29)

Project Manager approval authority requesting waiver of the above item:

_____

FIGURE 5–2

DESCRIPTION OF CIL WAIVER CODES

CODES

The requirements are coded as applicable to the following description of codes:

CODES	DESCRIPTION
1	Items not meeting the fail–safe requirement.
2	Items not meeting the redundancy verification requirement.
3	Items not meeting the fail–operational/fail–safe requirement.
4	Items not requiring PRCB approval and listed for information only. (These items do not require waiving.)
5	Items not meeting the GSE fail–safe requirement.
6	Items not meeting NSTS 08080–1 Design Standard 4B, 20A, or 32.
7	Items classified as Criticality 1R non–CILs not requiring retention rationale, but contained in the CIL for information to support ground turnaround and processing at KSC. (These items do not require waiving.)
E	Emergency systems/items failing in the emergency mode.
O	Criticality downgraded due to the consideration of defined and approved operational controls.
P	Loss of life other than crew (i.e., Criticality 1 failures which could result in loss of ground crew personnel or public).
*	Items not meeting the redundancy requirement during intact abort only.

NOTES

Alpha characters A, B, and C following either a Criticality 1R or 2R critical item indicate failure of a redundancy screen.

a. Redundancy screen A – Is the redundant item capable of checkout during normal ground turnaround?

b. Redundancy screen B – is loss of the redundant element readily detectable during flight?

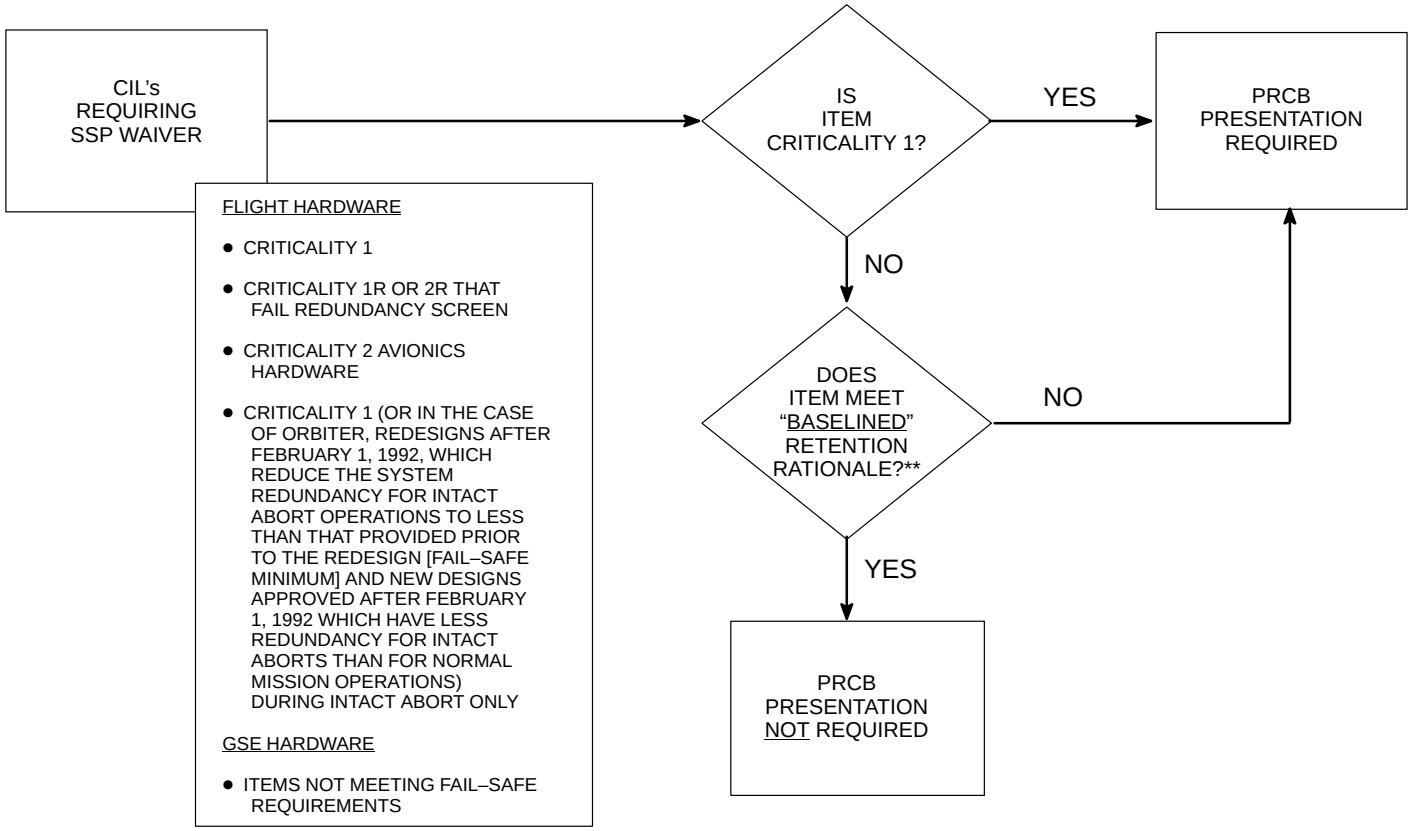
c. Redundancy screen C – Can loss of all redundant elements be caused by a single credible event, i.e., contamination, explosion, temperature, vibration, shock, acceleration, acoustics?

FIGURE 5–3 (DELETED)

FIGURE 5–4

CRITERIA FOR PRCB PRESENTATION

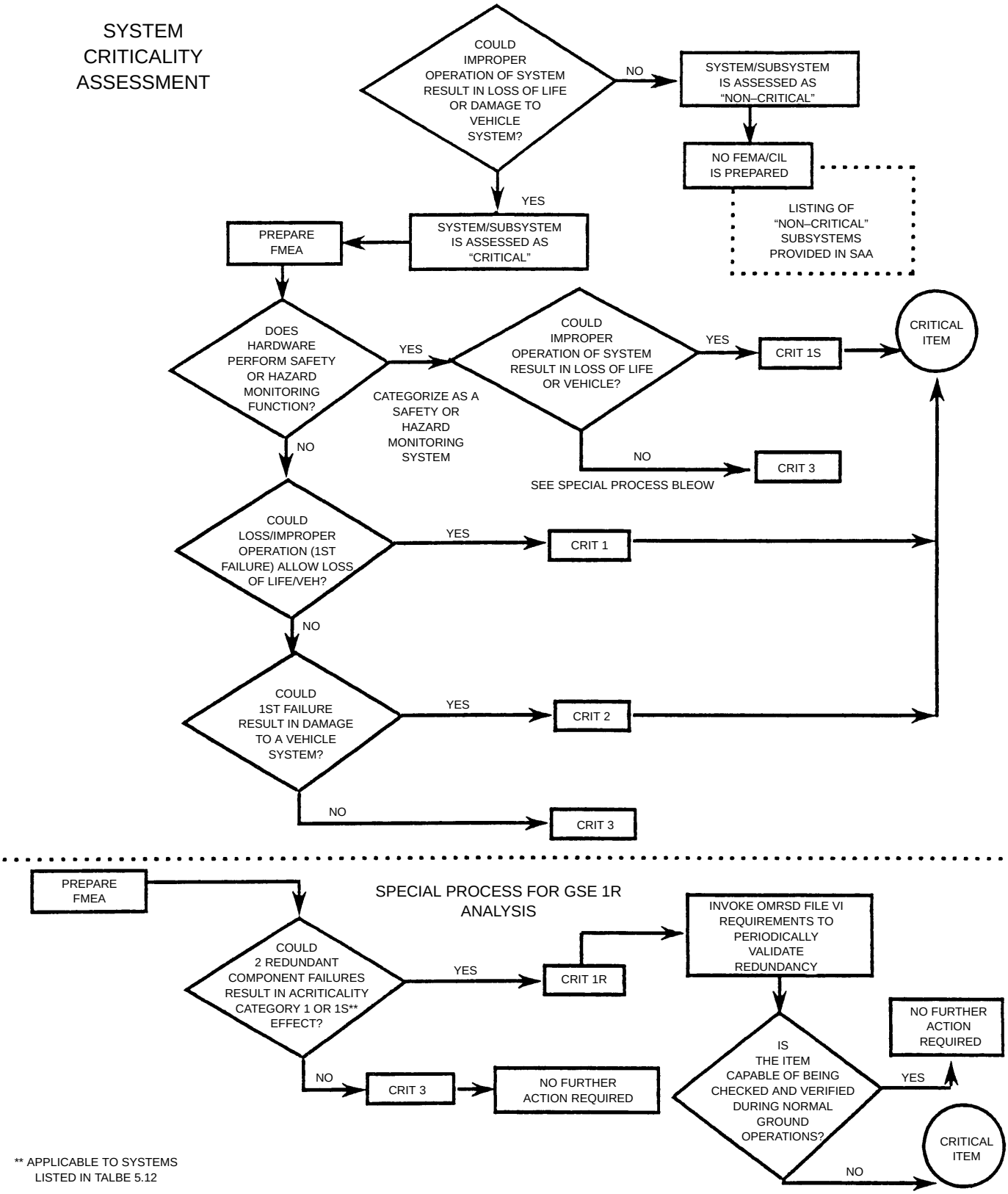
(FOR SPECIAL CLASSES OF HARDWARE ITEMS* HAVING SSP "BASELINED" GENERIC RETENTION RATIONALE
*SWITCHES, FILTERS, FLEX HOSES, BELLOWS, ORIFICES, POSITION INDICATORS, ETC.



**CIL ITEMS WHICH "BASELINED" RETENTION RATIONALE IS APPLICABLE, REQUIRE PREPARATION OF AN SSP WAIVER (CHANGE REQUEST). THIS IS NECESSARY TO MAINTAIN CONSISTENT APPLICATION OF SSP REDUNDANCY AND REDUNDANCY VERIFICATION REQUIREMENTS CONTAINED IN NSTS 07700, VOLUME X, AND DOCUMENTATION OF NONCOMPLIANCE WITH THOSE REQUIREMENTS.

FIGURE 5–5

GSE FMEA/CIL PROCESS



THIS PAGE INTENTIONALLY LEFT BLANK